Detailed Vulnerability Scan Report

Report Generated: December 15, 2015
Scan Completed: December 15, 2015 6:10 AM
Scan Level: heavy vulnerability
Scanner Version: 8.9.28

1 Details

The following sections provide details on the specific vulnerabilities detected on each host.

1.1 win2003unpatch.sainttest.local

IP Address: 10.8.0.11
Scan time: Dec 15 06:10:47 2015
Host type: Windows Server 2003
Netbios Name: WIN2003UNPATCH

vulnerable Microsoft.NET Framework version: 1.1.4322

Severity: Area of Concern
CVE: CVE-2007-0041 CVE-2007-0042 CVE-2007-0043

Updated 11/10/15

Impact

On a workstation, a remote attacker could execute arbitrary commands when a user opens a specially crafted web page. On a server, a remote attacker could cause a denial of service, execute arbitrary code, or gain unauthorized access to configuration files.

Background

The .NET Framework is a programming model for building Windows applications.

The Problem

Multiple vulnerabilities fixed by MS07-040

07/10/07
CVE 2007-0041
CVE 2007-0042
CVE 2007-0043
Microsoft Security Bulletin 07-040 fixed multiple vulnerabilities in the .NET Framework 1.0, 1.1, and 2.0, including a code execution vulnerability in the PE Loader service, an information disclosure vulnerability in ASP.NET allowing unauthorized access to configuration files, and a code execution vulnerability in the Just In Time compiler.

Resolution

Install the patch referenced in Microsoft Security Bulletins:

- 10-041 (.NET Framework 1.0, 1.1, 3.5)
- 11-039 (Silverlight 4)
- 11-069 (.NET Framework 3.5)
- 11-044 (.NET Framework 2.0, 3.5, 4.0)
- 11-066 (.NET Framework 3.5, 4.0)
- 12-035 (.NET Framework 1.1, 2.0, 3.5, 3.51, 4.0)
- 12-074 (.NET Framework 2.0, 3.5, 3.5.1, 4.0)
- 13-004
- 13-007 (.NET Framework 3.5, 3.5.1, 4.0)
- 13-015 (.NET Framework 2.0, 3.5, 3.5.1, 4.0, 4.5)
- 13-052 (.NET Framework 1.0, 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5)
- 13-082 (.NET Framework 2.0, 3.0, 3.5, 3.5.1, 4.0, 4.5)
- 14-046 (.NET Framework 2.0, 3.5, 3.5.1)
- 14-053 (.NET Framework 1.1, 2.0, 3.5, 3.5.1, 4.0, 4.5, 4.5.1, 4.5.2)

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-040, 09-036, 09-061, 10-041, 10-060, 11-028, 11-039, 11-044, 11-066, 11-069, 11-078, 11-100, 12-016, 12-025, 12-034, 12-035, 12-038, 12-074, 13-004, 13-007, 13-015, 13-040, 13-052, 13-082, 14-009, 14-026, 14-046, 14-053, 14-057, 14-059, 14-072, 15-041, 15-048, 15-044, 15-092, 15-101, 15-118.

Technical Details

Service: http
Sent: GET /s1a2i3n4.ashx HTTP/1.0
Host: win2003unpatch.sainttest.local
Received: X-AspNet-Version: 1.1.4322

Group Policy Code Execution Vulnerability (MS15-011)

Severity: Area of Concern **CVE:** CVE-2015-0008

Updated 12/08/15
CVE 1999-0662

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

Background

Microsoft releases updates for each of its Windows operating systems to fix a variety of problems which are discovered after the operating system is released. Some of these updates are released to address security issues which, if left unfixed, could have serious security implications.

There are three levels of updates released by Microsoft. *Hotfixes* are updates that fix a single issue or a few closely related issues. *Service Packs* (SP) are major updates of the operating system, which include all the hotfixes released since the last service pack. *Rollup Packages* are a collection of security hotfixes released since the last service pack. Rollup packages are used to ease the process of bringing a computer up to date in between the release of service packs.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
Group Policy Code Execution Vulnerability (MS15-011)	Fixes a code execution vulnerability that can be triggered when a user connects to a rogue network with a domain configured. (CVE 2015-0008)	**Vista:** KB3000483 KB3000483 (x64) **Windows Server 2008:** KB3000483 KB3000483 (x64) **Windows 7:** KB3000483 KB3000483 (x64) **Windows Server 2008 R2:** KB3000483 **Windows 8** KB3000483 KB3000483 (x64) **Windows 8.1** KB3000483 KB3000483 (x64) **Windows Server 2012** KB3000483 **Windows Server 2012 R2** KB3000483	15-011

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows XP, Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2, Windows 8.1, Windows 10, and Windows Server 2012 and Windows Server 2012 R2.

Technical Details

Service: netbios
No patch available for MS15-011 on Windows Server 2003

AV Information: Anti-virus software is not installed or its presence could not be checked

Severity: Potential Problem

Created 04/13/10

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Background

A virus is a self-replicating program designed to spread itself across a network. A computer can become infected with a virus when a user unknowingly installs it, usually by opening an untrustworthy e-mail attachment. Once installed, the virus takes some action to help itself propogate, and may take other actions, which are often harmless but sometimes malicious.

A worm is a self-replicating program designed to spread across a network without requiring any outside actions to take place. The main difference between a worm and a virus is that a virus relies on human actions, such as opening e-mail attachments or sharing files, to copy itself from one computer to another, whereas a worm is able to do so independently, allowing it to spread much faster.

There are many anti-virus products available which are designed to detect and eliminate viruses, worms, and other types of malware. These products work by checking files against a database of known malware patterns known as *signatures*. Typically, files are checked as they are accessed, and all files on the system are checked periodically.

Note that SAINT currently only collects information from the following AV software:

- McAfee 8.5
- Symantec
- AVG
- TrendMicro
- Forefront
- F-Secure

The Problem

If anti-virus software is not installed, enabled, or the database of anti-virus signatures is outdated, the system could be vulnerable to viruses, malware, and worms.

A last scan date that is not recent could mean that there are infected files on the system, especially if your anti-virus is disabled.

If logging is disabled in the anti-virus software, it could be hard to keep track of what was scanned at what time, as well as determining if anything is wrong with the software.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see Virus Bulletin.

Technical Details

Service: netbios
no registry access

Possible Microsoft IIS ASP Remote Code Execution vulnerability

Severity: Potential Problem **CVE:** CVE-2008-0075

Updated 09/14/10

Impact

An attacker could send a specially constructed request which crashes the server or executes arbitrary code with the privileges of the web server.

Background

Microsoft IIS web servers accept requests for a number of different types of files. The most common methods of requesting a file are **GET** and **POST**. In addition to the request itself, the web browser sends the IIS server additional information called *headers* which are not seen by the user. Information in the header can include browser type, content type, content length, and other information.

Some of the file types for which IIS may accept requests are **.HTR** files (for remote administration of passwords), **.IDC** files (Internet Database Connectors), **.STM** files (server side include files), **.PRINTER** files (printers), **.IDA** files (Internet Data Administration), **.IDQ** files (Internet Data Query), and **.ASP** files (Active Server Pages). Whenever any file of one of these types is requested by a client, a corresponding DLL file is executed on the server, regardless of whether or not the requested file actually exists on the server.

IIS supports *redirection*, which allows a user to specify that requests for a particular URL on the server should be redirected such that the user's browser loads a file from another directory, a network share, or a URL on another web server.

The Problems

ASP Remote Code Execution vulnerability

02/14/08
CVE 2008-0075
Microsoft Security Bulletin 08-006 announced a vulnerability in IIS that could allow remote code execution. The vulnerability exists in the way that IIS handles input to ASP Web pages. An attacker who could exploit the vulnerability could perform actions on the IIS server with the same rights as the Worker Process Identity (`WPI`).

Resolutions

Install the patches referenced in Microsoft Security Bulletins 03-018, 06-034 (for Windows 2000), 08-062, and 10-065.

For IIS 5.1, also install the patches referenced in 07-041. Note that the patch referenced in Microsoft Security Bulletin 02-050 must also be installed if client side certificates are to function.

IIS 4.0 users should also install the patch referenced in Microsoft Security Bulletin 04-021 or disable the *permanent redirection* option under the *Home Directory* tab in the web site properties.

Where can I read more about this?

More information on the ASP Remote Code Execution vulnerability in Windows 2003 and XP is available in Microsoft Security Bulletin 08-006, (US) CERT Technical Alert TA08-043C, Hewlett-Packard security bulletin HPSBST02314 / SSRT080016, Secunia advisory 28893, Security Focus Bugtraq ID 27676, and Security Tracker Alert ID 1019385.

Technical Details

Service: http
IIS 6 detected and cannot check for patch (credentials required)

Possible Microsoft IIS ASP Upload Command Execution vulnerability

Severity: Potential Problem **CVE:** CVE-2006-0026

Updated 09/14/10

Impact

An attacker could send a specially constructed request which crashes the server or executes arbitrary code with the privileges of the web server.

Background

Microsoft IIS web servers accept requests for a number of different types of files. The most common methods of requesting a file are **GET** and **POST**. In addition to the request itself, the web browser sends the IIS server additional information called *headers* which are not seen by the user. Information in the header can include browser type, content type, content length, and other information.

Some of the file types for which IIS may accept requests are **.HTR** files (for remote administration of passwords), **.IDC** files (Internet Database Connectors), **.STM** files (server side include files), **.PRINTER** files (printers), **.IDA** files (Internet Data Administration), **.IDQ** files (Internet Data Query), and **.ASP** files (Active Server Pages). Whenever any file of one of these types is requested by a client, a corresponding DLL file is executed on the server, regardless of whether or not the requested file actually exists on the server.

IIS supports *redirection*, which allows a user to specify that requests for a particular URL on the server should be redirected such that the user's browser loads a file from another directory, a network share, or a URL on another web server.

The Problems

ASP Upload Command Execution vulnerability

07/12/06
CVE 2006-0026
IIS 5.0, 5.1, and 6.0 are affected by a buffer overflow when processing ASP files. A remote attacker could execute arbitrary commands by uploading a specially crafted ASP file onto the web server, and then causing IIS to process it. An attacker would need to have valid login credentials in order to exploit this vulnerability unless the web server has been configured to allow anonymous uploads to the web site.

Resolutions

Install the patches referenced in Microsoft Security Bulletins 03-018, 06-034 (for Windows 2000), 08-062, and 10-065.

For IIS 5.1, also install the patches referenced in 07-041. Note that the patch referenced in Microsoft Security Bulletin 02-050 must also be installed if client side certificates are to function.

IIS 4.0 users should also install the patch referenced in Microsoft Security Bulletin 04-021 or disable the *permanent redirection* option under the *Home Directory* tab in the web site properties.

Where can I read more about this?

More information on the ASP Upload Command Execution vulnerability is available in Microsoft Security Bulletin 06-034, (US) CERT Vulnerability Note VU#395588, Neohapsis 2006 July message #0316, OSVDB record 27152, Secunia Advisory 21006, Security Focus Bugtraq ID 18858 and exploit, and Security Tracker Alert ID 1016466.

Technical Details

Service: http
IIS 6 detected and cannot check for patch (credentials required)

web server allows MIME sniffing

Severity: Potential Problem

Created 06/13/14

Impact

An attacker may be able to cause arbitrary script to run in a user's browser in the context of the vulnerable site.

Background

When rendering content from web servers, browsers need to know the type of content. For example, images need to be handled differently from HTML pages.

The content type is typically specified by the web server in the HTTP response headers. However, some browsers, in some situations, attempt to determine the content type by inspecting the content instead of relying on the response headers. This practice is known as *MIME sniffing*.

The Problem

MIME sniffing presents a cross-site scripting vulnerability when a file may be interpreted as a different file type by the server than by the browser. In particular, the server may consider the file to be non-executable, such as an image, while the browser considers the file to be executable. If the web site allows file uploads, this could allow an attacker to upload a specially crafted file which bypasses the server's MIME-type filters but contains script which executes when loaded in a browser.

Resolution

All HTTP responses should include an accurate **`Content-Type`** header, and an

`X-Content-Type-Options: nosniff` header. The latter header instructs browsers always to use the specified content type instead of performing MIME sniffing, and is currently supported by Internet Explorer and Chrome.

The **`X-Content-Type-Options: nosniff`** header can be set in the web server's configuration as follows:

- **Apache**:
  Add the following directive to the configuration file:

  ```
  Header set X-Content-Type-Options "nosniff"
  ```

- **IIS**:
  In IIS Manager, navigate to the desired level. Go to Features View -> HTTP Response Headers -> Actions pane. Click Add. In the Add Custom HTTP Response Header dialog box, enter **`X-Content-Type-Options`** in the *Name* box, and **`nosniff`** in the *Value* box.

Where can I read more about this?

For more information about MIME-sniffing risks and defenses, see Wikipedia and IE8 Security Part V. (Scroll down to the *MIME-Handling Changes* section.)

Technical Details

Service: http
Sent:
GET / HTTP/1.0
Host: win2003unpatch.sainttest.local
User-Agent: Mozilla/5.0
Received:
Missing Content-Type header or X-Content-Type-Options header not set to nosniff

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524
Created 04/14/08

Impact

A remote attacker could obtain sensitive information about the network.

Background

The Internet Control Message Protocol (ICMP) is a protocol used primarily for sending diagnostic messages and error messages between computers. The protocol defines a number of different message types, including echo requests and replies (used by the *ping* utility) and destination unreachable messages.

The Problem

CVE 1999-0524
ICMP defines a number of message types which disclose information about a computer. These message types were designed to help synchronize computers on a network, but in practice are rarely needed and should be disabled to prevent attackers from using them. Such message types include:

- *Timestamp requests*. These messages could be used by an attacker to determine the system's clock

state, which could be used to defeat authentication mechanisms which rely on certain pseudo-random number generators.
- *Netmask requests*. These messages could be used by an attacker to gather information about a network's subnet structure.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=91395e02

imap receives cleartext password

Severity: Potential Problem
Created 01/29/13

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the IMAP server.

Background

IMAP (Internet Message Access Protocol) is a protocol for accessing e-mail stored on a mail server. Unlike less sophisticated protocols such as POP, IMAP supports creation and management of mail folders to organize

messages on the server. A typical IMAP session begins with the IMAP client program sending a login name and password to the IMAP server using the **LOGIN** command.

The Problem

IMAP is a cleartext protocol. It does not require encryption between the client and server. Therefore, IMAP passwords and e-mail contents could be captured by an attacker, if the attacker is able to place a network sniffer somewhere between the client and the server.

Resolution

Disable the IMAP server and use a more secure protocol such as IMAPS. If IMAP cannot be disabled, restrict access using iptables or TCP Wrappers such that only addresses on a local, trusted network can connect.

Where can I read more about this?

For more information, see Protocols - The Problem With Cleartext.

Technical Details

Service: imap
Received:
* OK IMAPrev1
GET BAD Unknown or NULL command
BAD NULL COMMAND
QUIT BAD NULL COMMAND
BAD NULL COMMAND

Obsolete Windows Release: Windows Server 2003

Severity: Potential Problem
Updated 04/08/14

Impact

Security updates for the target's Windows release are no longer available, possibly leaving the target vulnerable to attacks.

Background

The Microsoft Support LifeCycle is roughly 10 years for each new product as of 2002.

The Problem

Obsolete versions of Windows could be vulnerable to a variety of security problems for which there are no available fixes.

Resolution

Systems should be upgraded to a supported version of Microsoft Windows (Windows Vista or higher).

Where can I read more about this?

The information found at Microsoft Support LifeCycle has been laid out in the "Timeline Of Windows" table at Microsoft Windows (Wikipedia).

Technical Details

Service: registry
Received: Server: Microsoft-IIS/6.0

pop receives password in clear

Severity: Potential Problem
Created 10/24/05

Summary

POP2 and **POP3** servers allow non-UNIX users to access their mail on a machine without logging in.

Impact

Unauthorized users and/or malicious users exploiting this vulnerability may be able to gain access to the target system.

Background

POP servers give PC and Macintosh users a way to receive mail through another machine. When connecting to a **POP** server, the client transmits the user's userid and password in clear text. Once the user has been authenticated, the user then can access their mail.

The Problem

Each time the client reconnects to the **POP** server, the user's userid and password are transmitted. Some client programs check the **POP** server every few minutes to check for the arrival of new mail. These frequent checks increase the possibility of the machine, username, and password being discovered by a password sniffer "tuned" for **POP** mail systems.

Resolution

The specification for **POP3** servers (RFC 1725) describes an optional command to help resolve this clear text password issue. When the initial connection is made to a **POP** server, the server displays a timestamp in its banner. The client uses this timestamp to create an MD5 hash string that is shared between the server and client. The next time the client connects to the server (e.g., to check for new mail) it will issue a command (**APOP**) and the hash string. This method reduces the number of times that a user's userid and password are transmitted in clear text.

An optional method (**IMAP4**), described in RFC 1734, provides another means of authentication. The AUTH command allows the client to specify an authentication mechanism to be used and a protocol exchange. This allows the client to specify authentication methods it knows about and challenge the server to see if it knows any of them as well. If no authentication method can be agreed upon, then the **APOP** command is used (RFC 1725).

Also, you may install the latest Secure **POP3** mail server (with **APOP**/**IMAP4**) or disable **POP** mail if necessary.

Where can I read more about this?

Read CERT Advisory 97.09 for more information on vulnerabilities found in IMAP and POP. Also, visit Eudora's Internet Messaging Primer for an overview on POP and IMAP.

Technical Details

Service: pop
Received: +OK POP3

SMTP receives cleartext password

Severity: Potential Problem
Created 09/05/14

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the mail server.

Background

The Simple Mail Transfer Protocol (SMTP) is used by a mail server to send, receive, or route e-mail across a network.

To prevent unauthorized use of mail servers, an extension to the SMTP protocol provides support for authentication. This is typically used to allow legitimate users to use a server for outgoing mail while preventing spammers from abusing the server.

When the SMTP authentication extension is enabled, servers typically support one or more authentication mechanisms. Several SMTP authentication mechanisms exist, such as LOGIN, PLAIN, CRAM-MD5, and NTLM.

The Problem

The SMTP service supports one or more authentication mechanisms which receive credentials in clear text. Therefore, SMTP passwords could be captured by an attacker, if the attacker is able to place a network sniffer somewhere between the client and the server.

Resolution

Disable the LOGIN and PLAIN authentication mechanisms as follows:

- **Postfix:** Set **`smtpd_sasl_security_options`** to **`noplaintext`** in the **`main.cf`** file.
- **Exchange:** In Exchange System Manager, expand Servers -> your inbound Exchange server -> Protocols -> SMTP. Right-click your inbound SMTP virtual server, and then click Properties. Go to the Access tab, and then Authentication, and clear the Basic Authentication check box.
- **Other mail servers:** Consult your mail server's documentation.

Where can I read more about this?

See RFC 2554 and the SMTP Authentication Tutorial for more information on SMTP authentication.

See the Microsoft article for more information about disabling Basic authentication in Microsoft Exchange.

Technical Details

Service: 587:TCP
Received:
250 AUTH LOGIN

SMTP receives cleartext password

Severity: Potential Problem

Created 09/05/14

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the mail server.

Background

The Simple Mail Transfer Protocol (SMTP) is used by a mail server to send, receive, or route e-mail across a network.

To prevent unauthorized use of mail servers, an extension to the SMTP protocol provides support for authentication. This is typically used to allow legitimate users to use a server for outgoing mail while preventing spammers from abusing the server.

When the SMTP authentication extension is enabled, servers typically support one or more authentication mechanisms. Several SMTP authentication mechanisms exist, such as LOGIN, PLAIN, CRAM-MD5, and NTLM.

The Problem

The SMTP service supports one or more authentication mechanisms which receive credentials in clear text. Therefore, SMTP passwords could be captured by an attacker, if the attacker is able to place a network sniffer somewhere between the client and the server.

Resolution

Disable the LOGIN and PLAIN authentication mechanisms as follows:

- **Postfix:** Set **`smtpd_sasl_security_options`** to **`noplaintext`** in the **`main.cf`** file.
- **Exchange:** In Exchange System Manager, expand Servers -> your inbound Exchange server -> Protocols -> SMTP. Right-click your inbound SMTP virtual server, and then click Properties. Go to the Access tab, and then Authentication, and clear the Basic Authentication check box.
- **Other mail servers:** Consult your mail server's documentation.

Where can I read more about this?

See RFC 2554 and the SMTP Authentication Tutorial for more information on SMTP authentication.

See the Microsoft article for more information about disabling Basic authentication in Microsoft Exchange.

Technical Details

Service: smtp
Received:
250 AUTH LOGIN

Web server default page detected

Severity: Potential Problem

Created 02/05/10

Impact

An unconfigured web server creates an unnecessary security exposure on the network.

Background

Many operating systems, such as Microsoft Windows and Linux, include web server software as either a default or optional package. The web server software usually includes a default web page. The default web page is the page that is served if a web client sends the web server a request before the web server has been configured.

The Problem

02/05/10 A web server containing a default web page is running. This indicates that the web server has not been configured, possibly because the owner of the target is not aware that web server software has been installed.

Unconfigured web servers create an unnecessary exposure and could contain potential security vulnerabilities.

Resolution

Disable unconfigured web servers. If the web server is needed, replace the default page with some appropriate site-specific content.

Where can I read more about this?

For more information about default web pages, see about.com.

Technical Details

Service: http
Received:
<title ID=titletext>Under Construction</title>

587/TCP

Severity: Service

Technical Details

220 WIN2003UNPATCH ESMTP

1026/UDP

Severity: Service

Technical Details

1027/UDP

Severity: Service

Technical Details

IMAP

Severity: Service

Technical Details

* OK IMAPrev1

POP

Severity: Service

Technical Details

+OK POP3

SMB

Severity: Service

Technical Details

\131\000\000\001\143

SMTP

Severity: Service

Technical Details

220 WIN2003UNPATCH ESMTP

WWW

Severity: Service

Technical Details

HTTP/1.1 200 OK
Content-Length: 1433
Content-Type: text/html
Content-Location: http://10.8.0.11/iisstart.htm
Last-Modified: Fri, 21 Feb 2003 23:48:30 GMT
Accept-Ranges:

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

1.2 xpprounpatched.sainttest.local

IP Address: 10.8.0.14
Scan time: Dec 15 06:10:46 2015

Host type: Windows 2000
Netbios Name: XPPROUNPATCHED

Microsoft Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)

Severity: Critical Problem **CVE:** CVE-2012-0002 CVE-2012-0152

Updated 12/08/15
CVE 1999-0662

Impact

The absence of critical updates leads to the potential for denial of service or unauthorized access by attackers or malicious web sites.

Background

Microsoft releases updates for each of its Windows operating systems to fix a variety of problems which are discovered after the operating system is released. Some of these updates are released to address security issues which, if left unfixed, could have serious security implications.

There are three levels of updates released by Microsoft. *Hotfixes* are updates that fix a single issue or a few closely related issues. *Service Packs* (SP) are major updates of the operating system, which include all the hotfixes released since the last service pack. *Rollup Packages* are a collection of security hotfixes released since the last service pack. Rollup packages are used to ease the process of bringing a computer up to date in between the release of service packs.

The Problems and Resolutions

One or more of the following security updates is not installed on the target system. The resolution is to install the needed updates. This can be done either by following the links in the table, or by visiting the Windows Update service which will automatically determine which updates are needed for your system and help you install them. It is a good idea to make a backup of the system before installing an update, especially for service packs. After the system has been brought up to date, check Microsoft's web site regularly for new

critical updates.

Note: The links below apply to the standard editions of Windows operating systems. If you are using a Terminal Server edition, a 64-bit edition, or a non-Intel edition which is not listed, consult the corresponding Microsoft Security Bulletins for patch information.

Update Name	Description	Fix	Bulletin
MS Remote Desktop Could Allow Remote Code Execution Vulnerabilities	Fixed Remote Code Execution Vulnerabilities in the Remote Desktop Protocol. If exploited, an attacker could run arbitrary code on the target system, then install programs; view, change, or delete data; or create new accounts with full user rights. (CVE 2012-0002, CVE 2012-0152)	KB2621440 and KB2621402 **XP:** 32-bit, 64-bit **2003:** 32-bit, 64-bit, Itanium **Vista:** 32-bit, 64-bit **2008:** 32-bit, 64-bit, Itanium **2008 R2:** 64-bit(1), 64-bit(2), Itanium(1), Itanium(2) **Win 7:** 32-bit(1), 32-bit(2), 64-bit(1), 64-bit(2)	12-020

Where can I read more about this?

For more information on critical updates, see the Windows critical update pages which are available for Windows XP, Windows Vista, Windows Server 2003, Windows 7, Windows Server 2008 and Windows Server 2008 R2, Windows 8.1, Windows 10, and Windows Server 2012 and Windows Server 2012 R2.

Technical Details

Service: 3389
rdp server allows connect to unfreed channels. No error code at byte eight.

AV Information: Anti-virus software is not installed or its presence could not be checked

Severity: Potential Problem

Created 04/13/10

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Background

A virus is a self-replicating program designed to spread itself across a network. A computer can become infected with a virus when a user unknowingly installs it, usually by opening an untrustworthy e-mail attachment. Once installed, the virus takes some action to help itself propogate, and may take other actions, which are often harmless but sometimes malicious.

A worm is a self-replicating program designed to spread across a network without requiring any outside actions to take place. The main difference between a worm and a virus is that a virus relies on human actions, such

as opening e-mail attachments or sharing files, to copy itself from one computer to another, whereas a worm is able to do so independently, allowing it to spread much faster.

There are many anti-virus products available which are designed to detect and eliminate viruses, worms, and other types of malware. These products work by checking files against a database of known malware patterns known as *signatures*. Typically, files are checked as they are accessed, and all files on the system are checked periodically.

Note that SAINT currently only collects information from the following AV software:

- McAfee 8.5
- Symantec
- AVG
- TrendMicro
- Forefront
- F-Secure

The Problem

If anti-virus software is not installed, enabled, or the database of anti-virus signatures is outdated, the system could be vulnerable to viruses, malware, and worms.

A last scan date that is not recent could mean that there are infected files on the system, especially if your anti-virus is disabled.

If logging is disabled in the anti-virus software, it could be hard to keep track of what was scanned at what time, as well as determining if anything is wrong with the software.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see Virus Bulletin.

Technical Details

Service: netbios
no registry access

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524

Created 04/14/08

Impact

A remote attacker could obtain sensitive information about the network.

Background

The Internet Control Message Protocol (ICMP) is a protocol used primarily for sending diagnostic messages and error messages between computers. The protocol defines a number of different message types, including echo requests and replies (used by the *ping* utility) and destination unreachable messages.

The Problem

CVE 1999-0524
ICMP defines a number of message types which disclose information about a computer. These message types were designed to help synchronize computers on a network, but in practice are rarely needed and should be disabled to prevent attackers from using them. Such message types include:

- *Timestamp requests*. These messages could be used by an attacker to determine the system's clock state, which could be used to defeat authentication mechanisms which rely on certain pseudo-random number generators.
- *Netmask requests*. These messages could be used by an attacker to gather information about a network's subnet structure.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=50ab6402

Possible vulnerability in Microsoft Terminal Server

Severity: Potential Problem

CVE: CVE-2000-1149 CVE-2001-0663 CVE-2001-0716 CVE-2002-0863 CVE-2002-0864 CVE-2005-1218

Updated 07/25/05

Impact

Vulnerabilities in Microsoft Windows Terminal Server and Remote Desktop could allow a remote attacker to execute arbitrary code or crash the server, or could allow an attacker who is able to capture network traffic to decrypt sessions.

Background

Windows 2000 and Windows NT 4.0 Terminal Server Edition feature Terminal Services, and Windows XP features a Remote Desktop service. These services allow use of Windows NT, 2000, and XP operating systems from platforms that otherwise could not run them, such as Win16, Macintosh, and Unix. Windows terminal clients communicate with the server using the Remote Desktop Protocol (**RDP**). **RDP** is used to send mouse and keystroke information to the server, and to send display information back to the client.

The Problems

RDP Denial of Service

07/25/05
CVE 2005-1218
A vulnerability in RDP could allow a remote attacker to cause a denial of service by sending the computer an invalid RDP packet. Windows 2000, Windows XP, and Windows Server 2003 are affected by this vulnerability.

RDP Encryption Weaknesses

04/15/03
All versions of RDP allow terminal sessions to be encrypted. However, two flaws are known to exist in the encryption implementation which could allow an attacker to recover the original plaintext session, and thus view sensitive information. Firstly, the RDP client accepts the public key sent to it by the server without any verification, leaving it susceptible to a man-in-the-middle attack. An attacker who is able to perform DNS spoofing or arp poisoning could act as a relay during the session's initial key exchange, leading to the ability to decrypt the entire session.

09/19/02
CVE 2002-0863
Secondly, the implementation of RDP in Windows 2000 and XP sends checksums generated from plaintext session data over the network unencrypted. These checksums could allow an attacker who is able to capture network traffic to recover the original plaintext session.

Invalid RDP data denial of service

09/19/02
10/26/01
CVE 2001-0663
CVE 2002-0864
Due to improper handling of a certain sequence of malformed **RDP** data, a remote attacker could cause the server to fail. The server would then need to be rebooted in order to resume normal operation. The attacker would not need to successfully establish a session with the server in order to exploit the vulnerability.

Windows XP with Remote Desktop enabled is affected by this vulnerability. Terminal servers running on either Windows NT 4.0 or Windows 2000 are affected by a similar but unrelated vulnerability.

Citrix MetaFrame denial of service

10/26/01
CVE 2001-0716
Citrix MetaFrame works with Windows terminal services to provide application server capabilities. Due to improper handling of multiple sessions by Citrix MetaFrame, it is possible for a remote attacker to crash the server by initiating a large number of fake sessions with the server, waiting for them to time out, and then initiating another new session. The server would then need to be rebooted in order to resume normal operation. The attacker would not need access to an account on the system in order to exploit the vulnerability.

Citrix MetaFrame 1.8 Server with Service Pack 3, Citrix MetaFrame XP Server, and Citrix MetaFrame XP Server with Service Pack 1 are affected by this vulnerability.

Windows NT 4.0 Terminal Server buffer overflow

CVE 2000-1149
A buffer overflow in the code that handles the terminal server's login prompt could allow a remote attacker to execute arbitrary code without logging in. This could allow the attacker to read, modify, or delete files, or upload programs and run them.

Windows NT 4.0 Terminal Server is affected by this vulnerability, unless the patch has been applied.

Resolution

There is no fix available to protect against the man-in-the-middle attack. Therefore, Terminal Services should only be used on trusted networks.

For Windows NT 4.0 Terminal Server Edition, apply the patches referenced in Microsoft Security Bulletins 00-087 and 01-052. There is no fix available for the denial of service vulnerability on Windows NT.

For Windows 2000, apply the patches referenced in Microsoft Security Bulletins 01-052, 02-051, and 05-041.

For Windows XP, apply the patches referenced in Microsoft Security Bulletins 02-051 and 05-041.

For Windows Server 2003, apply the patch referenced in Microsoft Security Bulletin 05-041.

For Citrix MetaFrame, download a hotfix from the Citrix Solution Knowledge Base, under *Hotfixes*.

It is also a good idea to filter TCP port 3389 at the firewall or router, such that only connections from legitimate users will be accepted.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 00-087, 01-052, 02-051, and 05-041, and Bugtraq.

For more information on the Citrix MetaFrame vulnerability, see the Bugtraq ID 3440.

Technical Details

Service: ms-wbt-server
port 3389/tcp open and KB899591 not applied or could not be checked

Microsoft Terminal Server allows weak encryption

Severity: Potential Problem

Created 07/01/13

Impact

An attacker who is able to monitor the network between the client and server could decrypt the desktop session.

Background

Microsoft Remote Desktop Services, formerly called Terminal Services, allow desktop sessions from remote clients over the network. Windows terminal clients communicate with the server using the Remote Desktop Protocol (**RDP**). **RDP** is used to send mouse and keystroke information to the server, and to send display information back to the client.

The RDP protocol supports multiple levels of encryption to help secure the session as it travels over the network.

The Problems

The Remote Desktop Service does not require clients to use strong encryption. A client could initiate a remote desktop session with 40- or 56-bit encryption, which could then be decrypted by an attacker who is able to capture packets between the client and server.

Resolution

From the Terminal Services Configuration application, change the *Encryption Level* setting in the connection's properties to *High*. This will require clients to use the maximum key strength.

Where can I read more about this?

For more information on securing remote desktop sessions, see Microsoft Article ID 816594.

Technical Details

Service: 3389
ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

1026/UDP

Severity: Service

Technical Details

SMB

Severity: Service

Technical Details

\131\000\000\001\143

WWW

Severity: Service

Technical Details

HTTP/1.1 400 Bad Request
Content-Type: text/html
Server: Microsoft-HTTPAPI/1.0
Date: Tue, 15 Dec 2015 10:59:50 GMT
Connection: close
Content-Length: 39
<h1>Bad Request

blackjack (1025/UDP)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

ssdp (1900/UDP)

Severity: Service

Technical Details

1.3 saintvm64.sainttest.local

IP Address: 10.8.0.35
Scan time: Dec 15 06:10:46 2015

Host type: Ubuntu 12.04
Netbios Name: SAINTVM64

vulnerability in Samba 3.6.3

Severity: Critical Problem

CVE: CVE-2012-1182 CVE-2012-2111 CVE-2013-0454 CVE-2013-4124 CVE-2013-4408 CVE-2013-4475 CVE-2013-4496 CVE-2014-0178 CVE-2014-0244 CVE-2014-3493 CVE-2014-8143 CVE-2015-0240

Updated 02/23/15

Impact

A remote attacker could create accounts, read part of the credentials file, execute arbitrary commands, cause a denial of service, write to arbitrary files, gain elevated privileges, or disable logging of failed login attempts in a brute-force password attack.

Background

Server Message Block (SMB) is a network protocol native to Windows systems which allows sharing of files and printers across a network. Samba is a software package which implements the **SMB** protocol on a variety of platforms, providing compatibility with Windows systems.

Every computer which uses the **SMB** protocol, is assigned a *NetBIOS name*. This name is used to identify the computer on the network for the purposes of resolving **SMB** requests.

Samba servers typically run two daemons: **smbd**, which provides SMB services, and **nmbd**, which provides name service which allows the server to appear in the Windows Network Neighborhood.

The Problems

Unexpected code execution in smbd

02/23/15
CVE 2015-0240
Samba versions 4.1.17, 4.0.25 and 3.6.25 fixed a vulnerability which could allow remote attackers to execute

arbitrary code with root privileges. The vulnerability exists due to a flaw in `srv_netlog_nt.c` when handling specially crafted sequence of packets following anonymous netlogon packet.

Active Directory Domain Controller Privilege Elevation

01/23/15
CVE 2014-8143
Samba versions 4.0.x before 4.0.24 and 4.1.x before 4.1.16 could allow remote authenticated users to set the `LDB userAccountControl UF_SERVER_TRUST_ACCOUNT` bit, when an Active Directory Domain Controller is configured. Successful exploitation could allow for elevation of privilege.

Samba Two Denial of Service Vulnerabilities

06/23/14
CVE 2014-0244
CVE 2014-3493
Samba versions prior to 3.6.24, 4.0.19, and 4.1.9 are prone to two vulnerabilities, which can be exploited to cause a DoS (Denial of Service). The vulnerabilities exist due to:

- An error in the `sys_recvfrom` function where a malformed packet can cause the nmbd server to loop the CPU.
- An error when handling Unicode file names. A valid unicode path names stored on disk can cause smbd to crash if an authenticated client attempts to read them using a non-unicode request.

Samba Uninitialized Memory Information Disclosure Vulnerability

05/30/14
CVE 2014-0178
Samba versions 3.6.6 through 4.1.7 are prone to a vulnerability, which can be exploited to disclose potentially sensitive information. The vulnerability can be exploited to retrieve eight bytes of uninitialized server memory when a shadow-copy VFS module is enabled.

Samba DCE-RPC Packets Handling Buffer Overflow Vulnerability

12/13/13
CVE 2013-4408
CVE 2013-4496
Samba versions prior to 3.6.22, 4.0.13, and 4.1.3 are prone to a vulnerability, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to incorrect checking of the DCE-RPC fragment length in the client code. The vulnerability can be exploited to cause a buffer overflow by providing a specially crafted fragment length field.

Samba Insecure File Permissions and Security Bypass Vulnerabilities

11/15/13
CVE 2013-4475
CVE 2013-4476
Samba versions prior to 3.6.20, 4.0.11, and 4.1.1 do not check the underlying file or directory access control list when opening an alternate data stream. This vulnerability can be exploited to disclose information such as contents of inaccessible alternate streams. In addition, Samba version prior to 4.0.11 and 4.1.1 creates private keys that are used for the SSL/TLS encryption for ldaps with insecure world-readable permissions. This vulnerability can be exploited by local users to obtain sensitive information by reading the key file.

Note:

- By default no version of Samba supports alternate data streams on files or directories.
- By default, the http(s) service is not started, only if the "server services" option contains "web".
- The ldap(s) service is only started if Samba is configured as an active directory domain controller.

Packet Handling Denial of Service Vulnerability

08/08/13
CVE 2013-4124
Samba before 3.5.22, 3.6.17, and 4.0.8 is prone to a vulnerability, which can be exploited to cause a DoS (Denial of Service). The vulnerability is caused due to an unspecified error when handling malformed packets and can be exploited to exhaust memory resources by sending a specially crafted packet.

Samba CIFS Attribute Handling Vulnerability

04/09/13
CVE 2013-0454
Samba before 3.6.6 is prone to a vulnerability, which can be exploited by malicious users to bypass certain security restrictions. The vulnerability is caused due to the attributes of Samba CIFS share not properly handled.

LSA RPC "take ownership" Privilege Security Bypass Vulnerability

05/03/12
CVE 2012-2111
Samba versions 3.4.x before 3.4.17, 3.5.x before 3.5.15, and 3.6.x before 3.6.5 are prone to a vulnerability, which can be exploited by malicious users to bypass certain security restrictions. The security issue is caused due to improper application of security checks in the `CreateAccount, OpenAccount, AddAccountRights, and RemoveAccountRights` remote procedure calls (RPC) within the Local Security Authority (LSA). This can be exploited to gain "take ownership" privileges and e.g. change the ownership of arbitrary files and directories on the `smdb` file server.

Unauthenticated remote code execution vulnerability

04/11/12
CVE 2012-1182
A vulnerability in Samba could allow remote, anonymous attackers to execute arbitrary code with root privileges. The problem occurs in generated code which controls marshalling and unmarshalling of RPC calls over the network, due to the use of a client-supplied length value when allocating the memory for an array.

Samba 3.6.3, 3.5.13, and 3.4.15 and earlier are affected by this vulnerability.

3.x Multiple Unspecified Remote Vulnerabilities

09/30/09
Samba 3.x is prone to multiple unspecified remote vulnerabilities, including:

- An error in 'smbd' that can be exploited to cause a heap-based overflow.
- An error when Samba is compiled with '--enable-developer' can lead to a heap-based overflow.
- Multiple unspecified stack overflows.
- An unspecified heap-based buffer overflow.

Attackers can exploit these issues to execute code within the context of the affected server. Failed exploit attempts will result in a denial-of-service condition.

Resolution

Upgrade to Samba 3.6.35 for 3.6.x, 4.0.25 for 4.0.x, 4.1.17 for 4.1.x, or higher when available.

Alternatively, apply a fix from your operating system vendor.

Where can I read more about this?

A list of all reported vulnerabilities affecting Samba is available from Samba.

The unexpected code execution in smbd was reported in Samba Security CVE-2015-0240.

The Active Directory Domain Controller Privilege Elevation was reported in Samba Security CVE-2014-8143.

The Samba two denial of service vulnerabilities were reported in Samba Security CVE-2014-0244 and Samba Security CVE-2014-3493.

The Samba uninitialized memory information disclosure vulnerability was reported in Samba Security CVE-2014-0178.

The Samba DCE-RPC packets handling buffer overflow vulnerability was reported in Secunia Advisory SA55966 and Samba Security CVE-2013-4496.

The Samba insecure file permissions and security bypass vulnerabilities were reported in Secunia Advisory SA55638.

The Packet Handling Denial of Service vulnerability was reported in Secunia Advisory SA54347.

The Samba CIFS attribute handling vulnerability was reported in Secunia Advisory SA52854.

The LSA RPC "take ownership" Privilege Security Bypass vulnerability was reported in Secunia Advisory SA48976.

The unauthenticated remote code execution vulnerability was reported in a Samba announcement.

The 3.x Multiple Unspecified Remote vulnerabilities were reported in Bugtraq ID 36250.

Technical Details

Service: netbios-ssn
Received: Samba 3.6.3

OpenSSH 5.9p1 is vulnerable

Severity: Area of Concern

CVE: CVE-2010-5107 CVE-2014-1692 CVE-2014-2532 CVE-2014-2653 CVE-2015-5352 CVE-2015-5600

Impact

Updated 09/04/15

Impact

This document describes some vulnerabilities in the OpenSSH cryptographic login program. Outdated versions of OpenSSH may allow a malicious user to log in as another user, to insert arbitrary commands into a session, or to gain remote root access to the OpenSSH server.

Background

Secure Shell, or **ssh**, is a program used to log into another computer over a network, execute commands on a remote machine and move files from one machine to another. It provides strong authentication and secure communications over unsecure communication channels. **ssh** is intended as a replacement for **rlogin**, **rsh** and **rcp**. Additionally, **ssh** provides secure **X** connections and secure forwarding of arbitrary **TCP** connections. Traditional BSD "r" commands, such as **rsh**, **rlogin** and **rcp**, are vulnerable to a variety of different hacker attacks. A user with "**root**" access to certain machines on the network, or physical access to the network itself, may be able to gain unauthorized access to systems by exploiting various vulnerabilities found in the BSD "r" commands. Also, it may be possible for a malicious user to log all traffic to and from a target system, including keystrokes and passwords. The **X Window System** also has a number of vulnerabilities which may be exploited by hackers. The use of **ssh** helps to correct these vulnerabilities. Specifically, **ssh** protects against these attacks: **IP spoofing** (where the spoofer is on either a remote or local host), **IP source routing**, **DNS spoofing**, interception of cleartext passwords/data and attacks based on listening to **X** authentication data and spoofed connections to an **X11** server.

OpenSSH is an open-source implementation of the **ssh** protocol. It was originally developed for OpenBSD but a portable version is available for other operating systems.

The Problems

OpenSSH keyboard-interactive authentication vulnerability

07/23/15
CVE 2015-5600
OpenSSH 6.9 and earlier are prone to a vulnerability, which can be exploited by malicious users to bypass the maximum number of authentication attempts and launch brute force attacks. Note: The vulnerability exists on systems that have keyboard-interactive authentication enabled by default.

XSECURITY restrictions bypass vulnerability

07/09/15
CVE 2015-5352
OpenSSH before 6.9 is prone to a vulnerability, which can be exploited by malicious users to bypass certain security restrictions. The vulnerability exists due to OpenSSH not checking refusal deadline in `x11_open_helper` function after `ForwardX11Timeout` expires.

OpenSSH Client Rejected `HostCertificate` Handling Vulnerability

06/26/14
CVE 2014-2653
OpenSSH before 6.6 is prone to a vulnerability, which can be exploited by malicious users to bypass certain security restrictions. The vulnerability exists due to OpenSSH client not checking SSHFP records if SSH server offers a `HostCertificate` that the SSH client doesn't accept.

OpenSSH Buffer Initialization Vulnerability

05/27/14
CVE 2014-1692

OpenSSH through 6.4, when Makefile.inc is modified to enable `J-PAKE` protocol, does not initialize certain data structures. Attackers may be able to cause denial of service through memory corruption, or may cause an error condition.

OpenSSH "`child_set_env()`" Security Bypass Vulnerability

03/24/14
CVE 2014-2532
OpenSSH before 6.6 is prone to a vulnerability, which can be exploited by malicious, local users to bypass certain security restrictions. The vulnerability exists due to an error in the "`child_set_env()`" function. The vulnerability can be exploited to bypass intended environment restrictions by using a substring before a wildcard character.

OpenSSH Connection Saturation Remote DoS Vulnerability

06/13/13
CVE 2010-5107
The default configuration of OpenSSH through 6.1 enforces a fixed time limit between establishing a TCP connection and completing a login (**`logingracetime`**). This makes it easier for remote attackers to cause a denial of service by periodically making many new TCP connections where the total number exceeds the **`maxstartup`** default threshold setting.

Resolution

Upgrade to OpenSSH version 7.1 or higher when available, or install a fix from your operating system vendor.

Where can I read more about this?

The OpenSSH keyboard-interactive authentication vulnerability was reported in OpenSSH Vulnerability Exposes Servers to Brute Force Attacks.

The XSECURITY restrictions bypass vulnerability was reported in OpenSSH Release 6.9.

The OpenSSH Client Rejected `HostCertificate` Handling Vulnerability and The OpenSSH "`child_set_env()`" Security Bypass Vulnerability were reported in DSA-2894-1.

The OpenSSH Connection Saturation Remote DoS vulnerability was reported in the oss-security list and as Bugtraq ID 58162.

Technical Details

Service: ssh

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524
Created 04/14/08

Impact

A remote attacker could obtain sensitive information about the network.

Background

The Internet Control Message Protocol (ICMP) is a protocol used primarily for sending diagnostic messages and error messages between computers. The protocol defines a number of different message types, including echo requests and replies (used by the *ping* utility) and destination unreachable messages.

The Problem

CVE 1999-0524
ICMP defines a number of message types which disclose information about a computer. These message types were designed to help synchronize computers on a network, but in practice are rarely needed and should be disabled to prevent attackers from using them. Such message types include:

- *Timestamp requests*. These messages could be used by an attacker to determine the system's clock state, which could be used to defeat authentication mechanisms which rely on certain pseudo-random number generators.
- *Netmask requests*. These messages could be used by an attacker to gather information about a network's subnet structure.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=02666c0e

NetBIOS share enumeration using null session

Severity: Potential Problem

Created 10/18/02

CVE 2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Background

Windows operating systems include a feature known as *null sessions*. A null session is a way of connecting to a remote Windows workstation or server without any user authentication. A null session grants limited privileges which allow other Windows systems to retrieve certain information which is required for Microsoft networking, but isn't intended to allow any type of access which could be exploited by an attacker.

The Problem

An attacker could establish a null session with the system and use it to gain information about the system, such as the names of shared folders, the host SID, and the domain SID. The SID can be used to list user account names, potentially leading to password guessing attacks.

Resolution

Mitigating this vulnerability will require editing the registry. The **`regedt32`** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **`HKEY_LOCAL_MACHINE`**
Key: **`SYSTEM/CurrentControlSet/Control/LSA`**
Value: **`RestrictAnonymous`**
Type: **`REG_DWORD`**

Setting this value to **`1`** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **`2`** for greater protection. However, a value of **`2`** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **`RestrictAnonymousSAM`**, which, if set to **`1`**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **`RestrictAnonymous`** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Shares: print$

Windows null session domain SID disclosure

Severity: Potential Problem **CVE:** CVE-2000-1200

Created 10/18/02
CVE 2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Background

Windows operating systems include a feature known as *null sessions*. A null session is a way of connecting to a remote Windows workstation or server without any user authentication. A null session grants limited privileges which allow other Windows systems to retrieve certain information which is required for Microsoft networking, but isn't intended to allow any type of access which could be exploited by an attacker.

The Problem

An attacker could establish a null session with the system and use it to gain information about the system, such as the names of shared folders, the host SID, and the domain SID. The SID can be used to list user account names, potentially leading to password guessing attacks.

Resolution

Mitigating this vulnerability will require editing the registry. The **`regedt32`** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **`HKEY_LOCAL_MACHINE`**
Key: **`SYSTEM/CurrentControlSet/Control/LSA`**
Value: **`RestrictAnonymous`**
Type: **`REG_DWORD`**

Setting this value to **`1`** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **`2`** for greater protection. However, a value of **`2`** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **`RestrictAnonymousSAM`**, which, if set to **`1`**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need

for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Domain SID = S-1-5-21-2796322588-1385680984-3600811486

Windows null session host SID disclosure

Severity: Potential Problem
Created 10/18/02
CVE 2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Background

Windows operating systems include a feature known as *null sessions*. A null session is a way of connecting to a remote Windows workstation or server without any user authentication. A null session grants limited privileges which allow other Windows systems to retrieve certain information which is required for Microsoft networking, but isn't intended to allow any type of access which could be exploited by an attacker.

The Problem

An attacker could establish a null session with the system and use it to gain information about the system, such as the names of shared folders, the host SID, and the domain SID. The SID can be used to list user account names, potentially leading to password guessing attacks.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Host SID = S-1-1459638016-4915282-5374023-5570639-80

excessive null session access

Severity: Potential Problem **CVE:** CVE-2000-1200

Created 10/18/02
CVE 2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Background

Windows operating systems include a feature known as *null sessions*. A null session is a way of connecting to a remote Windows workstation or server without any user authentication. A null session grants limited privileges which allow other Windows systems to retrieve certain information which is required for Microsoft networking, but isn't intended to allow any type of access which could be exploited by an attacker.

The Problem

An attacker could establish a null session with the system and use it to gain information about the system, such as the names of shared folders, the host SID, and the domain SID. The SID can be used to list user account names, potentially leading to password guessing attacks.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **`RestrictAnonymousSAM`**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **`RestrictAnonymous`** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Got user list: nobody

Remote OS available

Severity: Potential Problem
Created 05/27/08

Impact

The ability to detect which operating system is running on a machine enables attackers to be more accurate in attacks.

Background

Many systems include specific operating system information in the data which is returned when connecting to certain TCP ports. This data is known as the *banner* for a service.

The Problems

Remote OS available

05/27/08
This machine reveals its operating system type in the information which is returned when connecting to certain TCP ports. An attacker could use this information to choose attacks which specifically target the machine's operating system version, increasing the likelihood of success.

Resolution

Including the operating system in service banners is usually unnecessary. Therefore, change the banners of the services which are running on accessible ports. This can be done by disabling unneeded services, modifying the banner in a service's source code or configuration file if possible, or using TCP wrappers to modify the banner as described in the Red Hat Knowledgebase.

Where can I read more about this?

An example of ways to remove the Remote OS and other information is at my digital life.

Technical Details

Service: ssh
Received:
SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4

rpc.statd is enabled and may be vulnerable

Severity: Potential Problem

CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0210 CVE-1999-0493 CVE-2000-0666 CVE-2000-0800

Updated 02/11/11

Impact

Several vulnerabilities in **statd** permit attackers to gain root privileges. They can be exploited by local users. They can also be exploited remotely without the intruder requiring a valid local account if **statd** is accessible via the network.

Background

statd provides network status monitoring. It interacts with **lockd** to provide crash and recovery functions for the locking services on **NFS**.

The Problems

statd/automountd vulnerability

CVE 1999-0210
CVE 1999-0493

A vulnerability in **statd** allows an attacker to call arbitrary **rpc** services with the privileges of the **statd** process. This vulnerability could be used to exploit a second vulnerability in **automountd** which otherwise could only be exploited locally. The result is that the remote attacker could execute arbitrary commands.

Solaris, HP-UX, and IRIX 5.3 operating systems are affected by this vulnerability.

statd Buffer Overflow

CVE 1999-0018

Due to insufficient bounds checking on input arguments which may be supplied by local users, as well as remote users, it is possible to overwrite the internal stack space (where a program stores information to be used during its execution) of the **statd** program while it is executing a specific **rpc** routine. By supplying a carefully designed input argument to the **statd** program, intruders may be able to force **statd** to execute arbitrary commands as the user running **statd**. In most instances, that user will be **root**. This vulnerability can be exploited by local users. It can also be exploited remotely without the intruder requiring a valid local account if **statd** is accessible via the network.

Solaris versions prior to version 2.6, and some versions of IRIX, Digital Unix, and AIX are vulnerable. Check CERT Advisory 1997-26 to find out if your operating system is vulnerable.

String parsing error in `rpc.kstatd`

CVE 2000-0800

String parsing error in some packages of SuSE and possibly other Linux systems allows remote attackers to gain root privileges.

Format String Bug in statd

CVE 2000-0666

A format string bug in Linux versions of rpc.statd could allow remote root access. Linux (except OpenLinux) versions of rpc.statd prior to 0.1.9.1 are vulnerable.

`SM_MON` Request Buffer Overflow

A buffer overflow in the processing of **`SM_MON`** requests in the UnixWare version of **`statd`** could allow a remote attacker to gain access to the system. SCO UnixWare 7 is affected by this vulnerability.

File Creation or Removal using statd

CVE 1999-0019

Due to lack of input validation, the statd service could be used to create or delete files with root privileges. This vulnerability was publicized in April, 1996. Most operating systems which were available at that time are vulnerable. See CERT Advisory 1996-09 for information about your particular operating system.

Resolution

One resolution to this vulnerability is to install vendor patches as they become available. For the format string bug, SUSE users should obtain the **`nfs-utils`** and package, version 0.1.9.1 or higher, from their vendor. For the String parsing error bug, Linux users should obtain the **`nfs-utils`** or **`knfsdi`** or **`linuxnfs`** packages, more detail information, please refer to SUSE Security Announcement web site. For the **`SM_MON`** buffer overflow, UnixWare users should obtain the patch.

Also, if **`NFS`** is not being used, there is no need to run **`statd`** and it can be disabled. The **`statd`** (or **`rpc.statd`**) program is often started in the system initialization scripts (such as /etc/rc* or /etc/rc*.d/*). If you do not require **`statd`** it should be commented out from the initialization scripts. In addition, any currently running **`statd`** processes should be identified using **ps(1)** and then terminated using **kill(1)**.

Where can I read more about this?

More information about the **`statd/automountd`** vulnerability is available in CERT Advisory 1999-05. You may read more about the **`statd`** buffer overflow in CERT Advisory 1997-26. The String parsing error vulnerability detail information can be found in CVE Details. The format string vulnerability was discussed in vendor bulletins from Red Hat, Debian, Mandrake, Trustix, and Conectiva, as well as CERT Advisory 2000.17. The **`SM_MON`** buffer overflow was announced in Caldera Security Advisory 2001-SCO.6. The file creation and removal vulnerability was discussed in CERT Advisory 1996-09.

Technical Details

Service: 47152:TCP

SMB digital signing is disabled

Severity: Potential Problem

Created 03/26/12

Impact

If the SMB signing is disabled, malicious attackers could sniff the network traffic and could perform a man in the middle attack to gain sensitive information.

Background

The SMB protocol is the basis for Microsoft file and print sharing and other networking operations, such as remote Windows administration. Server Message Block (SMB) signing is a signature in the SMB protocol designed to help improve the security of the SMB protocol. See an SMB Protocol Package Exchange Scenario for better understanding.

The Problems

SMB Signing is disabled

03/26/12
Microsoft has put the SMB signing in SMB protocol as basis for the security setting. When this setting is disabled, the file and print sharing and other network operations are exposed to man in the middle attacks.

Resolution

Refer to Microsoft Technet Library in Local Policies, Microsoft network server: Digitally sign communications (if client agrees).

Where can I read more about this?

For more information about SMB signing configuration, see, SMB Protocol Package Exchange Scenario.

Technical Details

Service: netbios
NEGOTIATE_SECURITY_SIGNATURES_ENABLED=0

The sunrpc portmapper service is running

Severity: Potential Problem **CVE:** CVE-1999-0632

Created 09/01/11

Impact

The sunrpc portmapper service is an unsecured protocol that tells clients which port corresponds to each RPC service. Access to port 111 allows the calling client to query and identify the ports where the needed server is running.

Background

The portmapper program maps RPC program and version numbers to transport specific port numbers. The portmapper program currently supports two protocols UDP and TCP. The portmapper is contacted by talking to it on assigned port number 111 (SUNRPC) on either of these protocols.

The Problem

09/01/11
CVE 1999-0632
For systems that are unprotected and have portmapper running on port 111, a simple "rpcinfo -p" request will display program, version and services that are running.

Resolution

Disable all unnecessary RPC services, which are typically enabled in /etc/inetd.conf and in the system boot scripts, /etc/rc*, and to block high numbered ports at the network perimeter except for those which are needed.

Where can I read more about this?

More information can be obtained in, NVD for CVE-1999-0632.

Technical Details

Service: sunrpc
port 111/tcp is open

sunrpc services may be vulnerable

Severity: Potential Problem **CVE:** CVE-2002-0391 CVE-2003-0028

Updated 03/20/03
CVE 2002-0391
CVE 2003-0028

Impact

If an affected service is running, a remote attacker could execute arbitrary commands with *root* privileges.

Background

Sun's Remote Procedure Call package (known as RPC, or sunrpc) is used by a number of network services to communicate with programs on client hosts. It uses a protocol called External Data Representation (XDR) which allows RPC programs to transfer data in a format which is consistent across different platforms. RPC services usually run on high numbered TCP or UDP ports. There is also a *port mapper* service which tells clients which port corresponds to each RPC service.

The Problem

There are two vulnerabilities in Sun's RPC implementation, a buffer overflow in the **`xdr_array`** function and an integer overflow in the **`xdrmem_getbytes`** function. A remote attacker could execute arbitrary commands with *root* privileges by passing specially crafted input to a network service which uses either of these two functions.

Sun's libnsl library, BSD-derived libc libraries, and GNU C's glibc library 2.3.1 and earlier are affected by these vulnerabilities. Since **`xdr_array`** and **`xdrmem_getbytes`** are found in these libraries rather than a specific RPC program, any RPC service which uses these libraries could be affected. Additionally, any other services which use the XDR functions, such as OpenAFS and MIT Kerberos 5, could be affected.

Resolution

See CERT Advisories 2002-25 and 2003-10 for patch or upgrade information from your vendor. Note that it will be necessary to recompile statically linked applications after installing the patch or upgrade.

It would also be advisable to disable all unnecessary RPC services, which are typically enabled in **/etc/inetd.conf** and in the system boot scripts, **/etc/rc***, and to block high numbered ports at the network perimeter except for those which are needed. Of particular importance are **rpc.cmsd**, **dmispd**, and **kadmind**, which are known to be exploitable and should be disabled or blocked.

Where can I read more about this?

These vulnerabilities were reported in CERT Advisories 2002-25 and 2003-10.

Technical Details

Service: sunrpc

TCP timestamp requests enabled

Severity: Potential Problem

Created 06/26/08

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Background

The *Transmission Control Protocol* (TCP) is the protocol used by services such as **telnet**, **ftp**, and **smtp** to establish a connection between a client and a server. The **TCP** packet header includes an *option* field, which can hold zero or more options. One of those options is the *TCP timestamp*, which is used for round-trip time measurement. The value of the timestamp is obtained from a virtual clock which is proportional to real time.

The Problem

TCP timestamps are enabled on the remote host. This could allow a remote attacker to estimate the amount of time since the remote host was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

To disable TCP timestamps on Linux, add the following line to the **/etc/sysctl.conf** file:

```
net.ipv4.tcp_timestamps = 0
```

To disable TCP timestamps on Windows, set the following registry value:

Key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`
Value: `Tcp1323Opts`
Data: 0 or 1

To disable TCP timestamps on Cisco, use the following command:

```
no ip tcp timestamp
```

Where can I read more about this?

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

Technical Details

Service: sunrpc
timestamp=3044146913; uptime guess=141d 11h 58m 9s

password complexity policy disabled

Severity: Potential Problem **CVE:** CVE-1999-0535

Created 04/06/05 CVE 1999-0535
CVE 1999-0582

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Background

Microsoft operating systems have *account policies* which specify certain guidelines which are enforced for all users in a computer or domain. These policies can be used to improve security. The *minimum password length* and password complexity requirements help ensure that a password cannot be easily guessed or cracked. The *maximum password age* helps limit the opportunity for intruders to use compromised passwords by requiring users to change their password regularly. The *minimum password age* and *password history* limits re-use of passwords to ensure that users cannot defeat this security precaution. *Lockouts* hinder brute-force password guessing attacks by disabling an account for a period of time after a number of failed login attempts.

The Problem

One or more of the Windows account policy settings are weaker than the recommended settings. This leaves the system insufficiently protected from password attacks.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn

weak account lockout policy (0)

Severity: Potential Problem **CVE:** CVE-1999-0582

Created 04/06/05 CVE 1999-0535
CVE 1999-0582

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Background

Microsoft operating systems have *account policies* which specify certain guidelines which are enforced for all users in a computer or domain. These policies can be used to improve security. The *minimum password length* and password complexity requirements help ensure that a password cannot be easily guessed or cracked. The *maximum password age* helps limit the opportunity for intruders to use compromised passwords by requiring users to change their password regularly. The *minimum password age* and *password history* limits re-use of passwords to ensure that users cannot defeat this security precaution. *Lockouts* hinder brute-force password guessing attacks by disabling an account for a period of time after a number of failed login attempts.

The Problem

One or more of the Windows account policy settings are weaker than the recommended settings. This leaves the system insufficiently protected from password attacks.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn
0 > 3 or 0 = 0

weak minimum password age policy (0 days)

Severity: Potential Problem **CVE:** CVE-1999-0535
Created 04/06/05 CVE 1999-0535
CVE 1999-0582

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Background

Microsoft operating systems have *account policies* which specify certain guidelines which are enforced for all users in a computer or domain. These policies can be used to improve security. The *minimum password length* and password complexity requirements help ensure that a password cannot be easily guessed or cracked. The *maximum password age* helps limit the opportunity for intruders to use compromised passwords by requiring users to change their password regularly. The *minimum password age* and *password history* limits re-use of passwords to ensure that users cannot defeat this security precaution. *Lockouts* hinder brute-force password guessing attacks by disabling an account for a period of time after a number of failed login attempts.

The Problem

One or more of the Windows account policy settings are weaker than the recommended settings. This leaves the system insufficiently protected from password attacks.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and

Policies.

Technical Details

Service: netbios-ssn
0 < 2

weak minimum password length policy (5)

Severity: Potential Problem **CVE:** CVE-1999-0535

Created 04/06/05 CVE 1999-0535
CVE 1999-0582

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Background

Microsoft operating systems have *account policies* which specify certain guidelines which are enforced for all users in a computer or domain. These policies can be used to improve security. The *minimum password length* and password complexity requirements help ensure that a password cannot be easily guessed or cracked. The *maximum password age* helps limit the opportunity for intruders to use compromised passwords by requiring users to change their password regularly. The *minimum password age* and *password history* limits re-use of passwords to ensure that users cannot defeat this security precaution. *Lockouts* hinder brute-force password guessing attacks by disabling an account for a period of time after a number of failed login attempts.

The Problem

One or more of the Windows account policy settings are weaker than the recommended settings. This leaves the system insufficiently protected from password attacks.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn
5 < 8

weak password history policy (0)

Severity: Potential Problem **CVE:** CVE-1999-0535
Created 04/06/05 CVE 1999-0535
CVE 1999-0582

Impact

Weak password policies could make it easier for an attacker to gain unauthorized access to user accounts.

Background

Microsoft operating systems have *account policies* which specify certain guidelines which are enforced for all users in a computer or domain. These policies can be used to improve security. The *minimum password length* and password complexity requirements help ensure that a password cannot be easily guessed or cracked. The *maximum password age* helps limit the opportunity for intruders to use compromised passwords by requiring users to change their password regularly. The *minimum password age* and *password history* limits re-use of passwords to ensure that users cannot defeat this security precaution. *Lockouts* hinder brute-force password guessing attacks by disabling an account for a period of time after a number of failed login attempts.

The Problem

One or more of the Windows account policy settings are weaker than the recommended settings. This leaves the system insufficiently protected from password attacks.

Resolution

Edit the account policy, which is found in the *Local Security Policy* under *Administrative Tools* on most systems.

Change the account policy settings to the recommended values. In a typical organization, these are:

- Minimum password length: 8 characters
- Enforce password history: 24 passwords remembered
- Maximum password age: 42 days
- Minimum password age: 2 days
- Password complexity requirements: Enabled
- Account lockout threshold: 3 invalid logon attempts

Note that if there is an *Effective Setting* in the local security policy, it is this setting which is used. This setting can only be changed on the domain controller.

Where can I read more about this?

See Microsoft's Step-by-Step Guide to Enforcing Strong Password Policies and Account Passwords and Policies.

Technical Details

Service: netbios-ssn
0 < 24

SMB

Severity: Service

Technical Details

SSH

Severity: Service

Technical Details

SSH-2.0-OpenSSH_5.9p1 Debian-5ubuntu1.4

microsoft-ds (445/TCP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

sunrpc (111/TCP)

Severity: Service

Technical Details

sunrpc (111/UDP)

Severity: Service

Technical Details

1.4 10.8.0.38

IP Address: 10.8.0.38
Scan time: Dec 15 06:10:47 2015

Host type: Windows 7 SP1
Netbios Name: WIN7

vulnerable FileZilla server version: 0.9.41-beta

Severity: Area of Concern **CVE:** CVE-2014-0160 CVE-2014-0224

Updated 07/02/14

Impact

Vulnerabilities in FileZilla FTP server allow for a denial of service or attackers to obtain sensitive information.

Background

FileZilla FTP server is an FTP server for Windows.

The Problems

OpenSSL SSL/TLS Handshake Vulnerability

07/02/14
CVE 2014-0224
FileZilla Server before 0.9.45 is prone to a vulnerability, which can be exploited by an attacker to disclose potentially sensitive information and manipulate certain data. The vulnerability exists due to a bundled vulnerable OpenSSL version.

OpenSSL Vulnerability

05/16/14
CVE 2014-0160
FileZilla Server before 0.9.44 is affected by a vulnerability due to a bundled vulnerable OpenSSL version. The vulnerability could allow disclosure of portions of memory.

Resolution

Upgrade to version 0.9.45 or higher.

Where can I read more about this?

The OpenSSL SSL/TLS handshake vulnerability was reported in FileZilla Server Version 0.9.45.

The OpenSSL vulnerability was reported in FileZilla Server Version 0.9.44.

Technical Details

Service: ftp
Received: 220-FileZilla Server version 0.9.41 beta

AV Information: Anti-virus software is not installed or its presence could not be checked

Severity: Potential Problem

Created 04/13/10

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Background

A virus is a self-replicating program designed to spread itself across a network. A computer can become infected with a virus when a user unknowingly installs it, usually by opening an untrustworthy e-mail attachment. Once installed, the virus takes some action to help itself propogate, and may take other actions, which are often harmless but sometimes malicious.

A worm is a self-replicating program designed to spread across a network without requiring any outside actions to take place. The main difference between a worm and a virus is that a virus relies on human actions, such as opening e-mail attachments or sharing files, to copy itself from one computer to another, whereas a worm is able to do so independently, allowing it to spread much faster.

There are many anti-virus products available which are designed to detect and eliminate viruses, worms, and other types of malware. These products work by checking files against a database of known malware patterns known as *signatures*. Typically, files are checked as they are accessed, and all files on the system are checked periodically.

Note that SAINT currently only collects information from the following AV software:

- McAfee 8.5
- Symantec
- AVG
- TrendMicro
- Forefront
- F-Secure

The Problem

If anti-virus software is not installed, enabled, or the database of anti-virus signatures is outdated, the system could be vulnerable to viruses, malware, and worms.

A last scan date that is not recent could mean that there are infected files on the system, especially if your anti-virus is disabled.

If logging is disabled in the anti-virus software, it could be hard to keep track of what was scanned at what time, as well as determining if anything is wrong with the software.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see Virus Bulletin.

Technical Details

Service: netbios
no registry access

server is susceptible to BEAST attack

Severity: Potential Problem **CVE:** CVE-2011-3389

Created 10/28/11

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Background

Cipher Block Chaining (CBC) is an encryption mode of operation where the decryption of each block of encrypted text depends on all of the preceding blocks. CBC requires an Initialization Vector, a block of bits which starts the encryption and ensures that the encrypted text is unique. The SSLv3 and TLS 1.0 protocols may encrypt data using Cipher Block Chaining ciphers that use chained initialization vectors.

The Problem

SSL/TLS CBC Initialization Vector Prediction

10/28/11
CVE 2011-3389
The Browser Exploit against SSL/TLS (BEAST) may allow an attacker to perform a man-in-the-middle attack to obtain plain-text HTTP headers by conducting a blockwise chosen-boundary attack (BCBA) against an HTTPS session. This attack is an extension of two previously disclosed attacks against SSL. The first of these attacks was detailed by Gregory Bard in May 2004 (The Vulnerability of SSL to Chosen Plaintext Attack). This research showed that cipher block chaining mode used by SSL is vulnerable to decryption in cases where the attacker can control part of the plaintext. This attack proved to be difficult to implement against HTTPS sessions due to the attackers' inability to control the contents. This attack method was extended to support TLS 1.0 and improved in April 2006 (A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL).

In September 2011, Juliano Rizzo and Thai Duong presented a modern iteration of this attack that utilized Java or HTML5 WebSockets as an entry-point for attackers. Using this method, attackers could host a malicious website that, when visited by victims, uses Java or WebSockets to establish a connection to any secured 3rd party website of their choice. If the user has an active session to the targeted 3rd party site, any cookies he or she has saved will also be sent. Since the attacker is initiating this request, he can control the length of the requested resource, allowing him to position the cookie on a block boundary. The attacker also knows part of the cleartext. If this can be done in a man-in-the-middle scenario, the attacker will be able to intercept this encrypted request and decrypt it off-line to obtain the cookie. If the cookie contains an authentication token, this may result in account theft.

TLS 1.1 and later have been improved to use an explicit initialization vector strategy, rendering them immune to this type of attack.

Resolution

Most browser vendors have released updates which prevent this attack, but some affected browsers still remain at this time, so it is still advisable also to fix the problem on the server side. SSLv3 and TLS 1.0 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 and TLS 1.0 entirely on the server may affect the usability of the web site, as some web browsers may not yet support TLS 1.1, and therefore isn't recommended.

Where can I read more about this?

Thai Duong wrote a detailed blog post about this attack, including a video demonstration.
Adam Langley wrote a helpful blog post that helps highlight concerns for both browser vendors and website hosts.
Rob VanderBrink of SANS Internet Storm Center posted a blog update detailing TLS 1.1/1.2 support in many common browsers as of September, 2011.
Eric Rescorla wrote a detailed blog post explaining how the attack works in detail and analyzing the security impact of this vulnerability.

Technical Details

Service: ms-wbt-server
Server accepted TLS 1.0 CBC cipher: TLS_RSA_WITH_AES_128_CBC_SHA

server is susceptible to BEAST attack

Severity: Potential Problem **CVE:** CVE-2011-3389
Created 10/28/11

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Background

Cipher Block Chaining (CBC) is an encryption mode of operation where the decryption of each block of encrypted text depends on all of the preceding blocks. CBC requires an Initialization Vector, a block of bits which starts the encryption and ensures that the encrypted text is unique. The SSLv3 and TLS 1.0 protocols may encrypt data using Cipher Block Chaining ciphers that use chained initialization vectors.

The Problem

SSL/TLS CBC Initialization Vector Prediction

10/28/11
CVE 2011-3389
The Browser Exploit against SSL/TLS (BEAST) may allow an attacker to perform a man-in-the-middle attack to obtain plain-text HTTP headers by conducting a blockwise chosen-boundary attack (BCBA) against an HTTPS session. This attack is an extension of two previously disclosed attacks against SSL. The first of

these attacks was detailed by Gregory Bard in May 2004 (The Vulnerability of SSL to Chosen Plaintext Attack). This research showed that cipher block chaining mode used by SSL is vulnerable to decryption in cases where the attacker can control part of the plaintext. This attack proved to be difficult to implement against HTTPS sessions due to the attackers' inability to control the contents. This attack method was extended to support TLS 1.0 and improved in April 2006 (A Challenging but Feasible Blockwise-Adaptive Chosen-Plaintext Attack on SSL).

In September 2011, Juliano Rizzo and Thai Duong presented a modern iteration of this attack that utilized Java or HTML5 WebSockets as an entry-point for attackers. Using this method, attackers could host a malicious website that, when visited by victims, uses Java or WebSockets to establish a connection to any secured 3rd party website of their choice. If the user has an active session to the targeted 3rd party site, any cookies he or she has saved will also be sent. Since the attacker is initiating this request, he can control the length of the requested resource, allowing him to position the cookie on a block boundary. The attacker also knows part of the cleartext. If this can be done in a man-in-the-middle scenario, the attacker will be able to intercept this encrypted request and decrypt it off-line to obtain the cookie. If the cookie contains an authentication token, this may result in account theft.

TLS 1.1 and later have been improved to use an explicit initialization vector strategy, rendering them immune to this type of attack.

Resolution

Most browser vendors have released updates which prevent this attack, but some affected browsers still remain at this time, so it is still advisable also to fix the problem on the server side. SSLv3 and TLS 1.0 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 and TLS 1.0 entirely on the server may affect the usability of the web site, as some web browsers may not yet support TLS 1.1, and therefore isn't recommended.

Where can I read more about this?

Thai Duong wrote a detailed blog post about this attack, including a video demonstration.
Adam Langley wrote a helpful blog post that helps highlight concerns for both browser vendors and website hosts.
Rob VanderBrink of SANS Internet Storm Center posted a blog update detailing TLS 1.1/1.2 support in many common browsers as of September, 2011.
Eric Rescorla wrote a detailed blog post explaining how the attack works in detail and analyzing the security impact of this vulnerability.

Technical Details

Service: ftp
Server accepted SSLv3 CBC cipher: SSL3_CK_RSA_DES_192_CBC3_SHA

ftp receives cleartext password

Severity: Potential Problem

Created 01/29/13

Impact

Passwords could be stolen if an attacker is able to capture network traffic to and from the FTP server.

Background

File Transfer Protocol (FTP) is a TCP protocol for transmitting files over a network. A typical FTP session begins with the FTP client program sending a login name and password to the FTP server using the **USER** and **PASS** commands.

The Problem

FTP is a cleartext protocol. It does not require encryption between the client and server. Therefore, FTP passwords and file contents could be captured by an attacker, if the attacker is able to place a network sniffer somewhere between the client and the server.

Resolution

Disable the FTP server and use a more secure program such as SCP or SFTP to transfer files. If FTP cannot be disabled, restrict access using iptables or TCP Wrappers such that only addresses on a local, trusted network can connect.

Where can I read more about this?

For more information, see Protocols - The Problem With Cleartext.

Technical Details

Service: ftp
Received:
220-FileZilla Server version 0.9.41 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
500 Syntax error, command unrecognized.
221 Goodbye

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524

Created 04/14/08

Impact

A remote attacker could obtain sensitive information about the network.

Background

The Internet Control Message Protocol (ICMP) is a protocol used primarily for sending diagnostic messages and error messages between computers. The protocol defines a number of different message types, including echo requests and replies (used by the *ping* utility) and destination unreachable messages.

The Problem

CVE 1999-0524
ICMP defines a number of message types which disclose information about a computer. These message types were designed to help synchronize computers on a network, but in practice are rarely needed and should be disabled to prevent attackers from using them. Such message types include:

- *Timestamp requests*. These messages could be used by an attacker to determine the system's clock state, which could be used to defeat authentication mechanisms which rely on certain pseudo-random number generators.
- *Netmask requests*. These messages could be used by an attacker to gather information about a network's subnet structure.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=10e66602

Microsoft Terminal Server allows weak encryption

Severity: Potential Problem
Created 07/01/13

Impact

An attacker who is able to monitor the network between the client and server could decrypt the desktop session.

Background

Microsoft Remote Desktop Services, formerly called Terminal Services, allow desktop sessions from remote clients over the network. Windows terminal clients communicate with the server using the Remote Desktop Protocol (**RDP**). **RDP** is used to send mouse and keystroke information to the server, and to send display information back to the client.

The RDP protocol supports multiple levels of encryption to help secure the session as it travels over the network.

The Problems

The Remote Desktop Service does not require clients to use strong encryption. A client could initiate a remote desktop session with 40- or 56-bit encryption, which could then be decrypted by an attacker who is able to capture packets between the client and server.

Resolution

From the Terminal Services Configuration application, change the *Encryption Level* setting in the connection's properties to *High*. This will require clients to use the maximum key strength.

Where can I read more about this?

For more information on securing remote desktop sessions, see Microsoft Article ID 816594.

Technical Details

Service: 3389
ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

SMB digital signing is disabled

Severity: Potential Problem
Created 03/26/12

Impact

If the SMB signing is disabled, malicious attackers could sniff the network traffic and could perform a man in the middle attack to gain sensitive information.

Background

The SMB protocol is the basis for Microsoft file and print sharing and other networking operations, such as remote Windows administration. Server Message Block (SMB) signing is a signature in the SMB protocol designed to help improve the security of the SMB protocol. See an SMB Protocol Package Exchange Scenario for better understanding.

The Problems

SMB Signing is disabled

03/26/12
Microsoft has put the SMB signing in SMB protocol as basis for the security setting. When this setting is disabled, the file and print sharing and other network operations are exposed to man in the middle attacks.

Resolution

Refer to Microsoft Technet Library in Local Policies, Microsoft network server: Digitally sign communications (if client agrees).

Where can I read more about this?

For more information about SMB signing configuration, see, SMB Protocol Package Exchange Scenario.

Technical Details

Service: netbios
NEGOTIATE_SECURITY_SIGNATURES_ENABLED=0

server is susceptible to SSL POODLE attack

Severity: Potential Problem **CVE:** CVE-2014-3566

Updated 12/22/14

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Background

A *Block Cipher* is an encryption algorithm which operates on a fixed-size block of data. If the size of the data to be encrypted is not a multiple of the block size, then the data must be extended, or *padded*, with arbitrary bytes so that the last block is large enough to be encrypted.

Cipher Block Chaining (CBC) is an encryption mode of operation where the decryption of each block of encrypted text depends on all of the preceding blocks.

The Problem

SSL POODLE Attack

12/22/14
CVE 2014-8730
Only the SSLv3 protocol, and not the TLS protocol, is affected by this vulnerability. However, some TLS implementations, most notably in F5 and A10 devices, are known to be affected due to failure to enforce the protocol. Furthermore, even those clients and servers which correctly support TLS may still allow sessions to be downgraded to SSLv3 to allow compatibility with older peers. An attacker may be able to force this downgrade to occur by intercepting and modifying packets during the protocol negotiation phase, thus facilitating the POODLE attack.

10/15/14
CVE 2014-3566
The SSLv3 protocol, when used with CBC ciphers, is susceptible to an attack known as Padding Oracle On Downgraded Legacy Encryption (POODLE). The vulnerability arises because the padding is not deterministic

and is not covered by the Message Authentication Code (MAC) and therefore cannot be verified during decryption. This may allow an invalid, specially crafted stream of ciphertext to have a one in 256 chance of being accepted. Each time such a stream is accepted, one byte of the plaintext data can be inferred.

An attacker who is able to intercept SSL sessions (as in a man-in-the-middle attack) can exploit this vulnerability using javascript code which forces a user's browser to send HTTPS requests to a server, and then modifying these requests such that the desired plaintext byte is aligned with the end of a block. If this is done repeatedly, the desired plaintext byte will eventually become known, and the attacker can move on to the next byte, and then the next, until the desired plaintext (for example, the user's session ID) is known in its entirety.

Resolution

SSLv3 CBC ciphers should be disabled on the server as follows:

- **Apache:** Set the following directive in the Apache configuration file:

```
SSLCipherSuite RC4+RSA:!EXPORT:!LOW
```

- **IIS:** See See KB245030.

Note that disabling SSLv3 entirely is another alternative, but may affect the usability of the web site. The **TLS_FALLBACK_SCSV** mechanism can also be used to mitigate the vulnerability if it is supported by both the client and the server.

To fix the vulnerability in the TLS implementation in F5 devices, see SOL15882.

Where can I read more about this?

The POODLE attack was described in The POODLE Bites: Exploiting the SSL 3.0 Fallback.

The POODLE attack against TLS implementations was reported by ImperialViolet.

Technical Details

Service: ftp
Server accepted SSLv3 CBC cipher: SSL3_CK_RSA_DES_192_CBC3_SHA

SSL/TLS server supports RC4 ciphers

Severity: Potential Problem **CVE:** CVE-2013-2566 CVE-2015-2808
Created 04/28/15

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Background

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are encryption protocols used to ensure confidentiality as information travels across the Internet. They are commonly used between web browsers and web servers to protect sensitive data such as passwords and credit card numbers.

At the beginning of a TLS/SSL session, the client and server negotiate the encryption algorithm, known as a

cipher. RC4 (Rivest Cipher 4) is a stream cipher which is commonly used in TLS/SSL sessions.

The Problem

Invariance Weakness and Bar Mitzvah attack

04/28/15
CVE 2015-2808
Some RC4 keys contain a pattern which causes part of the state permutation to remain intact throughout the initialization process, resulting in leakage of plaintext bytes. This is known as the *Invariance Weakness*. This weakness can be used to partially decrypt TLS/SSL sessions which use affected keys in an attack known as *Bar Mitzvah*. An attacker would need to be able to sniff network traffic in order to exploit this vulnerability, and most RC4 keys do not have this weakness.

Ciphertext Bias Weakness

CVE 2013-2566
The encrypted stream which is output by the RC4 cipher contains small biases. This results in ciphertext which isn't truly random when the same plaintext is encrypted with different RC4 keys. This could make it easier for an attacker who can view network traffic to decrypt parts of the plaintext which are typically encrypted many types, such as browser cookies, ultimately leading to session hijacking.

Resolution

For Apache mod_ssl web servers, add **`!RC4`** to the **`SSLCipherSuite`** directive in the configuration file to disable RC4 ciphers.

For Microsoft IIS web servers, disable RC4 ciphers as described in Microsoft knowledge base article 245030.

For other types of web servers, consult the web server documentation to find out how to disable RC4 ciphers.

Where can I read more about this?

For more information on the Invariance Weakness and Bar Mitzvah attack, see Security Affairs and Imperva's paper, Attacking SSL when using RC4.

For more information on the ciphertext bias weakness, see the blog post Attack of the Week: RC4 is kind of broken in TLS.

Technical Details

Service: ftp
Server accepted SSL 3.0 RC4 cipher: SSL3_CK_RSA_RC4_128_MD5

SSL/TLS server supports RC4 ciphers

Severity: Potential Problem **CVE:** CVE-2013-2566 CVE-2015-2808
Created 04/28/15

Impact

A remote attacker with the ability to sniff network traffic could decrypt an encrypted session.

Background

Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are encryption protocols used to ensure confidentiality as information travels across the Internet. They are commonly used between web browsers and web servers to protect sensitive data such as passwords and credit card numbers.

At the beginning of a TLS/SSL session, the client and server negotiate the encryption algorithm, known as a *cipher*. RC4 (Rivest Cipher 4) is a stream cipher which is commonly used in TLS/SSL sessions.

The Problem

Invariance Weakness and Bar Mitzvah attack

04/28/15
CVE 2015-2808
Some RC4 keys contain a pattern which causes part of the state permutation to remain intact throughout the initialization process, resulting in leakage of plaintext bytes. This is known as the *Invariance Weakness*. This weakness can be used to partially decrypt TLS/SSL sessions which use affected keys in an attack known as *Bar Mitzvah*. An attacker would need to be able to sniff network traffic in order to exploit this vulnerability, and most RC4 keys do not have this weakness.

Ciphertext Bias Weakness

CVE 2013-2566
The encrypted stream which is output by the RC4 cipher contains small biases. This results in ciphertext which isn't truly random when the same plaintext is encrypted with different RC4 keys. This could make it easier for an attacker who can view network traffic to decrypt parts of the plaintext which are typically encrypted many types, such as browser cookies, ultimately leading to session hijacking.

Resolution

For Apache mod_ssl web servers, add **`!RC4`** to the **`SSLCipherSuite`** directive in the configuration file to disable RC4 ciphers.

For Microsoft IIS web servers, disable RC4 ciphers as described in Microsoft knowledge base article 245030.

For other types of web servers, consult the web server documentation to find out how to disable RC4 ciphers.

Where can I read more about this?

For more information on the Invariance Weakness and Bar Mitzvah attack, see Security Affairs and Imperva's paper, Attacking SSL when using RC4.

For more information on the ciphertext bias weakness, see the blog post Attack of the Week: RC4 is kind of broken in TLS.

Technical Details

Service: ms-wbt-server
Server accepted TLS 1.0 RC4 cipher: TLS_RSA_WITH_RC4_128_SHA

TCP timestamp requests enabled

Severity: Potential Problem
Created 06/26/08

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Background

The *Transmission Control Protocol* (TCP) is the protocol used by services such as **`telnet`**, **`ftp`**, and **`smtp`** to establish a connection between a client and a server. The **`TCP`** packet header includes an *option* field, which can hold zero or more options. One of those options is the *TCP timestamp*, which is used for round-trip time measurement. The value of the timestamp is obtained from a virtual clock which is proportional to real time.

The Problem

TCP timestamps are enabled on the remote host. This could allow a remote attacker to estimate the amount of time since the remote host was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

To disable TCP timestamps on Linux, add the following line to the **`/etc/sysctl.conf`** file:

```
net.ipv4.tcp_timestamps = 0
```

To disable TCP timestamps on Windows, set the following registry value:

Key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`
Value: `Tcp1323Opts`
Data: 0 or 1

To disable TCP timestamps on Cisco, use the following command:

```
no ip tcp timestamp
```

Where can I read more about this?

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

Technical Details

Service: netbios-ssn
timestamp=723408089; uptime guess=83d 17h 28m 0s

FTP

Severity: Service

Technical Details

220-FileZilla Server version 0.9.41 beta

SMB

Severity: Service

Technical Details

\131\000\000\001\143

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

microsoft-ds (445/TCP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

\022\003\001\003H\002\000\000F\003\001Vo\242\178\131C\182XN\247*\219&8\001
\005\012F\247\205\018\031\136\1724\242\152\237\217\004\253
\151\t\000\000\160\163~!\195\154;\212\158\222\183"7n9V\215HS\207\143\004}\207\221X\133\161\000
/\000\011\000\002\246\000\002\243\000\002\2400\130\002\2360\130\001\212\160\003\002\001\002\0
02\016\024\146\203\189\225\209c\143G@\246w\0186\153\1960\006\t*\134H\134\247\001\001\005\005\
0000\0311\0290\027\006\003U\004\003\019\020Win7.SAINTtest.local0\030\023150817183448Z\023160216
183448Z0\0311\0290\027\006\003U\004\003\019\020Win7.SAINTtest.local0\130\001"0\006\t*\134H\134\
247\001\001\001\005\000\003\130\001\015\0000\130\001

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

ssdp (1900/UDP)

Severity: Service

Technical Details

1.5 win-iqf3u12cja5.sainttest.local

IP Address: 10.8.0.150
Scan time: Dec 15 06:10:46 2015
Host type: Windows Server 2008 R2
Netbios Name: WIN-IQF3U12CJA5

DNS server allows zone transfers

Severity: Area of Concern **CVE:** CVE-1999-0532

Created 07/07/10
CVE 1999-0532

Impact

Attackers could collect information about the domain.

Background

A DNS zone transfer is the process by which a secondary name server copies all DNS records for a domain from a primary name server.

The Problems

If DNS zone transfers are not restricted, they can allow attackers to enumerate hosts in a domain.

Resolution

Configure the primary DNS server to allow zone transfers only from secondary DNS servers. In BIND, this can be done in an **`allow-transfer`** block in the **`options`** section of the **`named.conf`** file.

Where can I read more about this?

Information on DNS zone transfers can be found here.

Information on securing DNS can be found here.

Technical Details

Service: dns
Received:
; <<>> DiG 9.8.1-P1 <<>> @win-iqf3u12cja5.sainttest.local SAINTTEST.local axfr
; (1 server found)
;; global options: +cmd
SAINTTEST.local.\x093600\x09IN\x09SOA\x09win-iqf3u12cja5.SAINTTEST.local.
hostmaster.SAINTTEST.local. 4889 900 600 86400 3600
SAINTTEST.local.\x09600\x09IN\x09A\x0910.8.0.150
SAINTTEST.local.\x093600\x09IN\x09NS\x09win-iqf3u12cja5.SAINTTEST.local.
_gc._tcp.Default-First-Site-Name._sites.SAINTTEST.local. 600 IN\x09SRV 0 100 3268
win-iqf3u12cja5.sainttest.local.
_kerberos._tcp.Default-First-Site-Name._sites.SAINTTEST.local. 600 IN SRV 0 100 88
win-iqf3u12cja5.sainttest.local.

_ldap._tcp.Default-First-Site-Name._sites.SAINTTEST.local. 600 IN SRV 0 100 389 win-iqf3u12cja5.sainttest.local.
_gc._tcp.SAINTTEST.local. 600\x09IN\x09SRV\x090 100 3268 win-iqf3u12cja5.sainttest.local.
_kerberos._tcp.SAINTTEST.local.\x09600 IN\x09SRV\x090 100 88 win-iqf3u12cja5.sainttest.local.
_kpasswd._tcp.SAINTTEST.local. 600 IN\x09SRV\x090 100 464 win-iqf3u12cja5.sainttest.local.
_ldap._tcp.SAINTTEST.local. 600\x09IN\x09SRV\x090 100 389 win-iqf3u12cja5.sainttest.local.

NFS export list disclosure

Severity: Area of Concern

Created 07/09/10

Impact

A remote attacker could view the list of exported file systems, which may contain sensitive information about the target's file system and trusted hosts.

Background

In order to perform operations via the **NFS** network file system protocol, a client host sends **NFS** requests to the **NFS** server daemon with:

- an **NFS** file handle that specifies the target of the operation,
- the operation (lookup, read, write, change permissions), and
- the user on whose behalf the request is sent.

When an **NFS** client host wants to access a remote file system for the first time, it first needs to obtain an **NFS** file handle. To this end, the client host sends a mount request to the server's mount daemon. The server's mount daemon verifies that the client host has permission to access the requested file system. When the mount daemon grants access, it sends a (directory) file handle back to the **NFS** client.

The Problem

The target makes the list of exported file systems available to remote users without authentication. This allows an attacker to view the list. The list may contain the paths to the exported file systems, and the hosts which are allowed to mount them. This information could be helpful to an attacker in planning an attack.

Resolution

Disable the NFS service if it is not needed. If it is needed, block access to the mountd service at the firewall.

Where can I read more about this?

See Wikipedia for more information about NFS.

Technical Details

Service: 1048:TCP
Sent:
/sbin/showmount -e win-iqf3u12cja5.sainttest.local
Received:
Export list for win-iqf3u12cja5.sainttest.local:

Possible buffer overflow in Active Directory

Severity: Potential Problem

Updated 09/08/15

Impact

A remote attacker could crash the Active Directory service and force a reboot of the server. It may also be possible to execute commands on the server.

Background

Active Directory is the primary directory service offered by Windows servers. It allows centralized management and sharing of information on users and network resources, and acts as a central authority for network security. Active Directory is based on the Lightweight Directory Access Protocol (LDAP).

The Problem

Resolution

Install the patches referenced in Microsoft Security Bulletin 15-096.

Where can I read more about this?

For more information, see Microsoft Security Bulletins 07-039, 08-003, 08-035, 08-060, 09-018, 09-066, and 15-096.

Technical Details

Service: ldap

AV Information: Anti-virus software is not installed or its presence could not be checked

Severity: Potential Problem

Created 04/13/10

Impact

The system may be susceptible to viruses, worms, and other types of malware.

Background

A virus is a self-replicating program designed to spread itself across a network. A computer can become infected with a virus when a user unknowingly installs it, usually by opening an untrustworthy e-mail attachment. Once installed, the virus takes some action to help itself propogate, and may take other actions, which are often harmless but sometimes malicious.

A worm is a self-replicating program designed to spread across a network without requiring any outside actions to take place. The main difference between a worm and a virus is that a virus relies on human actions, such as opening e-mail attachments or sharing files, to copy itself from one computer to another, whereas a worm is able to do so independently, allowing it to spread much faster.

There are many anti-virus products available which are designed to detect and eliminate viruses, worms, and other types of malware. These products work by checking files against a database of known malware patterns known as *signatures*. Typically, files are checked as they are accessed, and all files on the system are checked periodically.

Note that SAINT currently only collects information from the following AV software:

- McAfee 8.5
- Symantec
- AVG
- TrendMicro
- Forefront
- F-Secure

The Problem

If anti-virus software is not installed, enabled, or the database of anti-virus signatures is outdated, the system could be vulnerable to viruses, malware, and worms.

A last scan date that is not recent could mean that there are infected files on the system, especially if your anti-virus is disabled.

If logging is disabled in the anti-virus software, it could be hard to keep track of what was scanned at what time, as well as determining if anything is wrong with the software.

Resolution

Install and enable anti-virus software. Turn on automatic updates and periodic scans. Enable logging.

If an anti-virus server or manager is present, make sure that all clients can communicate with it so that the client is as up to date as possible and can send crucial information to the master installation.

If more information is needed about the anti-virus software running on the network and a server or manager is present, it is a good place to look for information about the anti-virus clients.

If more than one instance of anti-virus software is installed on a system, remove all but one. Multiple anti-virus programs may interfere with each other and cause the system to run poorly.

Where can I read more about this?

For additional information about viruses and anti-virus products, see Virus Bulletin.

Technical Details

Service: netbios
no registry access

DNS server allows recursive queries

Severity: Potential Problem
Created 10/28/09

Impact

Allowing recursive queries may make the DNS server more susceptible to denial-of-service and cache poisoning attacks.

Background

The Domain Name System (DNS) translates host names to IP addresses using a network of servers. Any time an address needs to be resolved, such as when loading a URL in a web browser or sending an e-mail message, a query is typically sent to a nearby DNS server.

Recursion refers to the act of a nearby DNS server forwarding the request to another DNS server, based on the domain in the requested host name. The answer is then cached on the nearby DNS server, so that future requests for the same host name can be answered more quickly.

The Problem

The DNS server allows recursive queries, leading to two security concerns. Firstly, a spoofed DNS request could be used to flood an IP address with DNS responses from multiple servers, leading to a denial of service. Secondly, recursion increases the chances that an attacker could trick the server into believing that a fake DNS response came from a legitimate DNS server, leading to cache poisoning. The fake response could then be sent to any computer which uses the DNS server.

Resolution

Disable recursive queries on the DNS server.

For Windows DNS servers, this can be done by checking *Disable Recursion* from Start -> Control Panel -> Administrative Tools -> DNS -> Properties -> Advanced -> Server Options.

For BIND DNS servers, add the following line to the *options* section of the **`named.conf`** file:

```
recursion no;
```

Where can I read more about this?

For more information about the risks of recursive queries, see the Go Daddy Help Center.

Technical Details

Service: domain
Recursion Available flag = 1

ICMP timestamp requests enabled

Severity: Potential Problem **CVE:** CVE-1999-0524

Created 04/14/08

Impact

A remote attacker could obtain sensitive information about the network.

Background

The Internet Control Message Protocol (ICMP) is a protocol used primarily for sending diagnostic messages and error messages between computers. The protocol defines a number of different message types, including echo requests and replies (used by the *ping* utility) and destination unreachable messages.

The Problem

CVE 1999-0524
ICMP defines a number of message types which disclose information about a computer. These message types were designed to help synchronize computers on a network, but in practice are rarely needed and should be disabled to prevent attackers from using them. Such message types include:

- *Timestamp requests*. These messages could be used by an attacker to determine the system's clock state, which could be used to defeat authentication mechanisms which rely on certain pseudo-random number generators.
- *Netmask requests*. These messages could be used by an attacker to gather information about a network's subnet structure.

Resolution

Configure the system or firewall not to allow ICMP timestamp requests (message type 13) or ICMP netmask requests (message type 17). Instructions for doing this on specific platforms are as follows:

Windows:
Block these message types using the Windows firewall as described in Microsoft TechNet.

Linux:
Use ipchains or iptables to filter ICMP netmask requests using the command:

```
ipchains -A input -p icmp --icmp-type address-mask-request -j DROP
```

Use ipchains or iptables to filter ICMP timestamp requests using the commands:

```
ipchains -A input -p icmp --icmp-type timestamp-request -j DROP
ipchains -A output -p icmp --icmp-type timestamp-reply -j DROP
```

To ensure that this change persists after the system reboots, put the above command into the system's boot-up script (typically **`/etc/rc.local`**).

Cisco:
Block ICMP message types 13 and 17 as follows:

```
deny icmp any any 13
deny icmp any any 17
```

Where can I read more about this?

For more information about ICMP, see RFC792.

Technical Details

Service: icmp
timestamp=d00d7002

Is your LDAP secure?

Severity: Potential Problem
Updated 03/18/03

Impact

If an application uses a vulnerable implementation of LDAP, an attacker could cause a denial of service or execute arbitrary commands.

Background

A directory service is used to keep track of network entities such as files, applications, printers, and users. The Lightweight Directory Access Protocol (**LDAP**) is one protocol which can be used to access directory services. Many applications, such as mail servers, enterprise servers, and databases, use **LDAP** to provide directory access while conserving resources.

The Problem

03/18/03
Many implementations of the **LDAP** protocol do not properly handle requests which do not adhere to the expected format. Among the problems which may be present are buffer overflow conditions, format string vulnerabilities, and mishandling of requests which violate encoding rules. Exploitation of these problems could lead to denial of service or unauthorized access.

The following applications contain an implementation of **LDAP** which contains such vulnerabilities if unpatched:

- **iPlanet Directory Server** version 5.0 Beta and versions up to and including 4.13 (CVE 2001-1306 CVE 2001-1307 CVE 2001-1308)
- **IBM SecureWay**, certain versions running under Solaris and Windows 2000 (CVE 2001-1309 CVE 2001-1310)
- **Lotus Domino Servers** (Enterprise, Application, and Mail), R5 prior to 5.0.7a and (*03/18/03*) R6 prior to 6.0 Gold (CVE 2001-1311 CVE 2001-1312 CVE 2001-1313)
- **Critical Path LiveContent Directory**, version 8A.3 (CVE 2001-1314 CVE 2001-1315)
- **Critical Path InJoin Directory Server**, versions 3.0, 3.1, and 4.0 (CVE 2001-1314 CVE 2001-1315)
- **Teamware Office** for Windows NT and Solaris, prior to version 5.3ed1 (CVE 2001-1316 CVE 2001-1317)
- **Qualcomm Eudora WorldMail** for Windows NT, version 2 (CVE 2001-1318)
- **Microsoft Exchange 5.5** LDAP Service (Hotfix pending) (CVE 2001-1319)
- **Network Associates PGP Keyserver 7.0**, prior to Hotfix 2 (CVE 2001-1320)
- **Oracle Internet Directory**, versions 2.1.1.x and 3.0.1 (CVE 2001-0974 CVE 2001-0975 CVE 2001-1321)
- **OpenLDAP**
    - Version 1.x prior to 1.2.12 and 2.x prior to 2.0.8 (CVE 2001-0977)
    - *12/13/02* Additional vulnerabilities in version 2.x prior to 2.1.9 (CVE 2002-1378 CVE 2002-1379)

Resolution

See CERT Advisory 2001-18 for information on obtaining a patch for your application. OpenLDAP 2.x users may also need to fix a separate set of vulnerabilities which were reported in SuSE Security Announcement 2002:047. Consult your vendor for a fix.

If a patch is not available, then ports 389 and 636, TCP and UDP, should be blocked at the network perimeter until a patch can be applied.

Where can I read more about this?

For more information, see CERT Advisory 2001-18 and SuSE Security Announcement 2002:047.

Technical Details

Service: ldap

Windows null session domain SID disclosure

Severity: Potential Problem **CVE:** CVE-2000-1200

Created 10/18/02

CVE 2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Background

Windows operating systems include a feature known as *null sessions*. A null session is a way of connecting to a remote Windows workstation or server without any user authentication. A null session grants limited privileges which allow other Windows systems to retrieve certain information which is required for Microsoft networking, but isn't intended to allow any type of access which could be exploited by an attacker.

The Problem

An attacker could establish a null session with the system and use it to gain information about the system, such as the names of shared folders, the host SID, and the domain SID. The SID can be used to list user account names, potentially leading to password guessing attacks.

Resolution

Mitigating this vulnerability will require editing the registry. The **`regedt32`** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **`HKEY_LOCAL_MACHINE`**
Key: **`SYSTEM/CurrentControlSet/Control/LSA`**
Value: **`RestrictAnonymous`**
Type: **`REG_DWORD`**

Setting this value to **`1`** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **`2`** for greater protection. However, a value of **`2`** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be thoroughly tested.

Windows XP and later also support a registry value called **`RestrictAnonymousSAM`**, which, if set to **`1`**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or

gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Domain SID = S-1-5-21-1092970315-2611599247-3581362680

Windows null session host SID disclosure

Severity: Potential Problem
Created 10/18/02
CVE 2000-1200

Impact

A remote attacker could gain a list of shared resources or user names on the system.

Background

Windows operating systems include a feature known as *null sessions*. A null session is a way of connecting to a remote Windows workstation or server without any user authentication. A null session grants limited privileges which allow other Windows systems to retrieve certain information which is required for Microsoft networking, but isn't intended to allow any type of access which could be exploited by an attacker.

The Problem

An attacker could establish a null session with the system and use it to gain information about the system, such as the names of shared folders, the host SID, and the domain SID. The SID can be used to list user account names, potentially leading to password guessing attacks.

Resolution

Mitigating this vulnerability will require editing the registry. The **regedt32** command can be used for this purpose. Keep in mind that erroneous changes to the registry could leave the system in an unstable and unbootable state, so use due caution and have a working system backup and repair disk before editing the registry.

The privileges of null sessions can be limited by changing the following registry value:

Hive: **HKEY_LOCAL_MACHINE**
Key: **SYSTEM/CurrentControlSet/Control/LSA**
Value: **RestrictAnonymous**
Type: **REG_DWORD**

Setting this value to **1** will partially limit the amount of information which is available through a null session, but will still allow access to some sensitive information, including the user account list. On Windows 2000 and XP, this value can also be set to **2** for greater protection. However, a value of **2** could also disable some critical Windows networking functions, so this setting is recommended only for Internet servers, and should be

thoroughly tested.

Windows XP and later also support a registry value called **RestrictAnonymousSAM**, which, if set to **1**, prevents enumeration of accounts using a null session.

In addition to the above changes, it is also advisable to block access to the NetBIOS ports at the firewall or gateway router. There is usually no reason why a user outside the local network would have a legitimate need for NetBIOS access. NetBIOS runs on ports 135, 137, 138, and 139 (TCP and UDP).

Where can I read more about this?

For more information about using the **RestrictAnonymous** registry value to limit the privileges of null sessions, see Microsoft Knowledge Base articles Q143474 and Q246261.

Technical Details

Service: netbios-ssn
Host SID = S-1-5-21-1092970315-2611599247-3581362680

Microsoft Terminal Server allows weak encryption

Severity: Potential Problem

Created 07/01/13

Impact

An attacker who is able to monitor the network between the client and server could decrypt the desktop session.

Background

Microsoft Remote Desktop Services, formerly called Terminal Services, allow desktop sessions from remote clients over the network. Windows terminal clients communicate with the server using the Remote Desktop Protocol (**RDP**). **RDP** is used to send mouse and keystroke information to the server, and to send display information back to the client.

The RDP protocol supports multiple levels of encryption to help secure the session as it travels over the network.

The Problems

The Remote Desktop Service does not require clients to use strong encryption. A client could initiate a remote desktop session with 40- or 56-bit encryption, which could then be decrypted by an attacker who is able to capture packets between the client and server.

Resolution

From the Terminal Services Configuration application, change the *Encryption Level* setting in the connection's properties to *High*. This will require clients to use the maximum key strength.

Where can I read more about this?

For more information on securing remote desktop sessions, see Microsoft Article ID 816594.

Technical Details

Service: 3389
ENCRYPTION_LEVEL_CLIENT_COMPATIBLE

rpc.statd is enabled and may be vulnerable

Severity: Potential Problem

CVE: CVE-1999-0018 CVE-1999-0019 CVE-1999-0210 CVE-1999-0493 CVE-2000-0666 CVE-2000-0800

Updated 02/11/11

Impact

Several vulnerabilities in **statd** permit attackers to gain root privileges. They can be exploited by local users. They can also be exploited remotely without the intruder requiring a valid local account if **statd** is accessible via the network.

Background

statd provides network status monitoring. It interacts with **lockd** to provide crash and recovery functions for the locking services on **NFS**.

The Problems

statd/automountd vulnerability

CVE 1999-0210
CVE 1999-0493

A vulnerability in **statd** allows an attacker to call arbitrary **rpc** services with the privileges of the **statd** process. This vulnerability could be used to exploit a second vulnerability in **automountd** which otherwise could only be exploited locally. The result is that the remote attacker could execute arbitrary commands.

Solaris, HP-UX, and IRIX 5.3 operating systems are affected by this vulnerability.

statd Buffer Overflow

CVE 1999-0018

Due to insufficient bounds checking on input arguments which may be supplied by local users, as well as remote users, it is possible to overwrite the internal stack space (where a program stores information to be used during its execution) of the **statd** program while it is executing a specific **rpc** routine. By supplying a carefully designed input argument to the **statd** program, intruders may be able to force **statd** to execute arbitrary commands as the user running **statd**. In most instances, that user will be **root**. This vulnerability can be exploited by local users. It can also be exploited remotely without the intruder requiring a valid local account if **statd** is accessible via the network.

Solaris versions prior to version 2.6, and some versions of IRIX, Digital Unix, and AIX are vulnerable. Check CERT Advisory 1997-26 to find out if your operating system is vulnerable.

String parsing error in rpc.kstatd

CVE 2000-0800

String parsing error in some packages of SuSE and possibly other Linux systems allows remote attackers to

gain root privileges.

Format String Bug in statd

CVE 2000-0666

A format string bug in Linux versions of rpc.statd could allow remote root access. Linux (except OpenLinux) versions of rpc.statd prior to 0.1.9.1 are vulnerable.

SM_MON Request Buffer Overflow

A buffer overflow in the processing of **SM_MON** requests in the UnixWare version of **statd** could allow a remote attacker to gain access to the system. SCO UnixWare 7 is affected by this vulnerability.

File Creation or Removal using statd

CVE 1999-0019

Due to lack of input validation, the statd service could be used to create or delete files with root privileges. This vulnerability was publicized in April, 1996. Most operating systems which were available at that time are vulnerable. See CERT Advisory 1996-09 for information about your particular operating system.

Resolution

One resolution to this vulnerability is to install vendor patches as they become available. For the format string bug, SUSE users should obtain the **nfs-utils** and package, version 0.1.9.1 or higher, from their vendor. For the String parsing error bug, Linux users should obtain the **nfs-utils** or **knfsdi** or **linuxnfs** packages, more detail information, please refer to SUSE Security Announcement web site. For the **SM_MON** buffer overflow, UnixWare users should obtain the patch.

Also, if **NFS** is not being used, there is no need to run **statd** and it can be disabled. The **statd** (or **rpc.statd**) program is often started in the system initialization scripts (such as /etc/rc* or /etc/rc*.d/*). If you do not require **statd** it should be commented out from the initialization scripts. In addition, any currently running **statd** processes should be identified using **ps(1)** and then terminated using **kill(1)**.

Where can I read more about this?

More information about the **statd/automountd** vulnerability is available in CERT Advisory 1999-05. You may read more about the **statd** buffer overflow in CERT Advisory 1997-26. The String parsing error vulnerability detail information can be found in CVE Details. The format string vulnerability was discussed in vendor bulletins from Red Hat, Debian, Mandrake, Trustix, and Conectiva, as well as CERT Advisory 2000.17. The **SM_MON** buffer overflow was announced in Caldera Security Advisory 2001-SCO.6. The file creation and removal vulnerability was discussed in CERT Advisory 1996-09.

Technical Details

Service: 1039:TCP

The sunrpc portmapper service is running

Severity: Potential Problem **CVE:** CVE-1999-0632

Created 09/01/11

Impact

The sunrpc portmapper service is an unsecured protocol that tells clients which port corresponds to each RPC

service. Access to port 111 allows the calling client to query and identify the ports where the needed server is running.

Background

The portmapper program maps RPC program and version numbers to transport specific port numbers. The portmapper program currently supports two protocols UDP and TCP. The portmapper is contacted by talking to it on assigned port number 111 (SUNRPC) on either of these protocols.

The Problem

09/01/11
CVE 1999-0632
For systems that are unprotected and have portmapper running on port 111, a simple "rpcinfo -p" request will display program, version and services that are running.

Resolution

Disable all unnecessary RPC services, which are typically enabled in /etc/inetd.conf and in the system boot scripts, /etc/rc*, and to block high numbered ports at the network perimeter except for those which are needed.

Where can I read more about this?

More information can be obtained in, NVD for CVE-1999-0632.

Technical Details

Service: sunrpc
port 111/tcp is open

sunrpc services may be vulnerable

Severity: Potential Problem **CVE:** CVE-2002-0391 CVE-2003-0028

Updated 03/20/03
CVE 2002-0391
CVE 2003-0028

Impact

If an affected service is running, a remote attacker could execute arbitrary commands with *root* privileges.

Background

Sun's Remote Procedure Call package (known as RPC, or sunrpc) is used by a number of network services to communicate with programs on client hosts. It uses a protocol called External Data Representation (XDR) which allows RPC programs to transfer data in a format which is consistent across different platforms. RPC services usually run on high numbered TCP or UDP ports. There is also a *port mapper* service which tells clients which port corresponds to each RPC service.

The Problem

There are two vulnerabilities in Sun's RPC implementation, a buffer overflow in the **`xdr_array`** function and an integer overflow in the **`xdrmem_getbytes`** function. A remote attacker could execute arbitrary commands

with *root* privileges by passing specially crafted input to a network service which uses either of these two functions.

Sun's libnsl library, BSD-derived libc libraries, and GNU C's glibc library 2.3.1 and earlier are affected by these vulnerabilities. Since **`xdr_array`** and **`xdrmem_getbytes`** are found in these libraries rather than a specific RPC program, any RPC service which uses these libraries could be affected. Additionally, any other services which use the XDR functions, such as OpenAFS and MIT Kerberos 5, could be affected.

Resolution

See CERT Advisories 2002-25 and 2003-10 for patch or upgrade information from your vendor. Note that it will be necessary to recompile statically linked applications after installing the patch or upgrade.

It would also be advisable to disable all unnecessary RPC services, which are typically enabled in **`/etc/inetd.conf`** and in the system boot scripts, **`/etc/rc*`**, and to block high numbered ports at the network perimeter except for those which are needed. Of particular importance are **`rpc.cmsd`**, **`dmispd`**, and **`kadmind`**, which are known to be exploitable and should be disabled or blocked.

Where can I read more about this?

These vulnerabilities were reported in CERT Advisories 2002-25 and 2003-10.

Technical Details

Service: sunrpc

TCP timestamp requests enabled

Severity: Potential Problem

Created 06/26/08

Impact

A remote attacker could possibly determine the amount of time since the computer was last booted.

Background

The *Transmission Control Protocol* (TCP) is the protocol used by services such as **`telnet`**, **`ftp`**, and **`smtp`** to establish a connection between a client and a server. The **`TCP`** packet header includes an *option* field, which can hold zero or more options. One of those options is the *TCP timestamp*, which is used for round-trip time measurement. The value of the timestamp is obtained from a virtual clock which is proportional to real time.

The Problem

TCP timestamps are enabled on the remote host. This could allow a remote attacker to estimate the amount of time since the remote host was last booted.

Resolution

TCP timestamps are generally only useful for testing, and support for them should be disabled if not needed.

To disable TCP timestamps on Linux, add the following line to the **`/etc/sysctl.conf`** file:

```
net.ipv4.tcp_timestamps = 0
```

To disable TCP timestamps on Windows, set the following registry value:

Key: `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters`
Value: `Tcp1323Opts`
Data: 0 or 1

To disable TCP timestamps on Cisco, use the following command:

```
no ip tcp timestamp
```

Where can I read more about this?

More information on TCP timestamps and round-trip time measurement is available in RFC1323 and Microsoft Article 224829.

Technical Details

Service: https
timestamp=49450038; uptime guess=5d 17h 21m 40s

Windows DNS Server RPC Management Interface Buffer Overflow

Severity: Potential Problem **CVE:** CVE-2007-1748
Updated 12/08/15

Impact

The Windows DNS Server has a vulnerability that allows for remote code execution.

Background

Microsoft Windows implements the Domain Name System as a service. It also runs a Management Interface on a dynamically chosen port. Remote Procedure Calls (RPC) can be used to access this Management Interface.

The Problems

DNS Server RPC Management Interface Buffer Overflow

04/16/07
CVE 2007-1748
The Microsoft Windows Domain Name System (DNS) Server service has a stack buffer overflow vulnerability. This vulnerability is due to a boundary error while handling specially crafted Remote Procedure Call (RPC) requests. Successful exploitation of the vulnerability would allow for arbitrary code injection and execution in the security context of the affected RPC Server Service, commonly System.

Resolution

Apply the patch referenced in Microsoft Security Bulletin 15-127.

Windows Server 2008 and Windows Server 2008 R2 users should apply the patch referenced in Microsoft Security Bulletin 09-008.

For the management interface buffer overflow, remote management over RPC can be disabled by setting the value of `RpcProtocol` in `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DNS\Parameters` to 4. Setting this value to 0 will disable all DNS RPC functionality and will protect against both local and remote attempts to exploit the vulnerability.

Where can I read more about this?

For more information on specific vulnerabilities, see Microsoft Security Bulletins 07-029, 07-062, 09-008, 11-058, 12-017, and 15-127. The DNS server RPC management interface buffer overflow was reported in US-CERT Vulnerability Note VU#555920 and Secunia Advisory SA24871.

Technical Details

Service: 135:TCP
Windows DNS Server port open

DNS

Severity: Service

Technical Details

NFS

Severity: Service

Technical Details

1048:TCP

SMB

Severity: Service

Technical Details

\131\000\000\001\143

WWW

Severity: Service

Technical Details

HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 15 Dec 2015 10:59:51 GMT
Connection: close
Content-Length:

WWW (Secure)

Severity: Service

Technical Details

WWW (non-standard port 8082)

Severity: Service

Technical Details

HTTP/1.1 503 Service Unavailable
Content-Type: text/html; charset=us-ascii
Server: Microsoft-HTTPAPI/2.0
Date: Tue, 15 Dec 2015 10:59:51 GMT
Connection: close
Content-Length:

domain (53/UDP)

Severity: Service

Technical Details

epmap (135/TCP)

Severity: Service

Technical Details

isakmp (500/UDP)

Severity: Service

Technical Details

kerberos (88/TCP)

Severity: Service

Technical Details

kerberos (88/UDP)

Severity: Service

Technical Details

ldap (389/TCP)

Severity: Service

Technical Details

ldap (389/UDP)

Severity: Service

Technical Details

microsoft-ds (445/TCP)

Severity: Service

Technical Details

ms-wbt-server (3389/TCP)

Severity: Service

Technical Details

msft-gc (3268/TCP)

Severity: Service

Technical Details

msft-gc-ssl (3269/TCP)

Severity: Service

Technical Details

netbios-dgm (138/UDP)

Severity: Service

Technical Details

netbios-ns (137/UDP)

Severity: Service

Technical Details

ntp (123/UDP)

Severity: Service

Technical Details

ssl-ldap (636/TCP)

Severity: Service

Technical Details

sunrpc (111/TCP)

Severity: Service

Technical Details

sunrpc (111/UDP)

Severity: Service

Technical Details

unicall (4343/TCP)

Severity: Service

Technical Details

Scan Session: Office vuln scan; Scan Policy: heavy vulnerability; Scan Data Set: 15 December 2015 06:10