meta

Report generated by Nessus ™ Thu, 23 Aug 2023 16:07:42 EDT

RESUILTS

Vulnerabilities

- 20007 (2) - SSL Version 2 and 3 Protocol Detection
- 32321 (2) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
- 11356 (1) - NFS Exported Share Information Disclosure
- 32314 (1) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
- 33850 (1) - Unix Operating System Unsupported Version Detection
- 46882 (1) - UnrealIRCd Backdoor Detection
- 51988 (1) - Bind Shell Backdoor Detection
- 61708 (1) - VNC Server 'password' Password
- 70728 (1) - Apache PHP-CGI Remote Code Execution
- 125855 (1) - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
- 42873 (2) - SSL Medium Strength Cipher Suites Supported (SWEET32)
- 10205 (1) - rlogin Service Detection
- 10245 (1) - rsh Service Detection
- 19704 (1) - TWiki 'rev' Parameter Arbitrary Command Execution
- 36171 (1) - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-200
- 39469 (1) - CGI Generic Remote File Inclusion
- 42256 (1) - NFS Shares World Readable
- 59088 (1) - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
- 90509 (1) - Samba Badlock Vulnerability
- 136769 (1) - ISC BIND Service Downgrade / Reflected DoS
- 15901 (2) - SSL Certificate Expiry
- 45411 (2) - SSL Certificate with Wrong Hostname
- 51192 (2) - SSL Certificate Cannot Be Trusted
- 57582 (2) - SSL Self-Signed Certificate
- 65821 (2) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)
- 104743 (2) - TLS Version 1.0 Protocol Detection

192.168.60.101

12	11	37	10	143
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Wed Aug 23 16:07:42 2023

End time : Thu Aug 23 16:14:06 2023

Host Information

Netbios Name : METASPLOITABLE

IP: 192.168.60.101

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

70728 - Apache PHP-CGI Remote Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution .

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP CGI program.This could be abused to execute arbitrary code , reveal PHP source code , cause a system crash , etc.

Solution

Upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

Plugin output
tcp/80/www

20007 (2) - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/25/smtp)
192.168.60.101 (tcp/5432/postgresql)

32321 (2) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Synopsis

The remote SSL certificate uses a weak key.

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack .

Solution

Consider all cryptographic material generated on the remote host to be guessable . In particuliar , all SSH, SSL and OpenVPN key material should be re generated .

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/25/smtp)

192.168.60.101 (tcp/5432/postgresql)

11356 (1) - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host .

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host . An attacker may be able to leverage this to read (and possibly write) files on remote host .

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares .

Risk Factor

Critical

Plugin Output

192.168.60.101 (udp/2049/rpc-nfs)

11356 (1) - NFS Exported Share Information Disclosure

Synopsis

It is possible to access NFS shares on the remote host .

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host . An attacker may be able to leverage this to read (and possibly write) files on remote host .

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares .

Risk Factor

Critical

Plugin Output

192.168.60.101 (udp/2049/rpc-nfs)

32314 (1) - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak .

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library .

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack .

Solution

Consider all cryptographic material generated on the remote host to be guessable . In particuliar , all SSH, SSL and OpenVPN key material should be re generated .

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/22/ssh)

33850 (1) - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

Description

According to its self reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Solution

Upgrade to a version of the Unix operating system that is currently supported.

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/0)

46882 (1) - UnrealIRCd Backdoor Detection

Synopsis

The remote IRC server contains a backdoor.

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD 5 / SHA1 checksums, and re-install it.

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/6667/irc)

51988 (1) - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised .

Description

A shell is listening on the remote port without any authentication being required An attacker may use it by connecting to the remote port and sending commands directly .

Solution

Verify if the remote host has been compromised and reinstall the system if necessary.

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/1524/wild_shell)

61708 (1) - VNC Server 'password' Password

Synopsis

A VNC server running on the remote host is secured with a weak password .

Description

The VNC server running on the remote host is secured with a weak password Nessus was able to login using VNC authentication and a password of 'password'. A remote , unauthenticated attacker could exploit this to take control of the system .

Solution

Secure the VNC service with a strong password .

Risk Factor

Critical

Plugin Output

192.168.60.101 (tcp/5900/vnc)

125855 (1) - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

Synopsis

The remote web server hosts a PHP application that is affected by SQLi vulnerability.

Description

According to its self-reported version number, the phpMyAdmin application hosted on the remote web server is prior to 4.8.6. It is, therefore, affected by a SQL injection (SQLi) vulnerability that exists in designer feature of phpMyAdmin. An unauthenticated remote attacker can exploit this to inject or manipulate SQL queries in the back-end database, resulting in the disclosure or manipulation of arbitrary data.

Note that Nessus has not attempted to exploit these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to phpMyAdmin version 4.8.6 or later.

Alternatively, apply the patches referenced in the vendor advisories.

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/80/www)

42873 (2) - SSL Medium Strength Cipher Suites Supported (SWEET32)

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)
192.168.60.101 (tcp/5432/postgresql)

10205 (1) - rlogin Service Detection

Synopsis

The rlogin service is running on the remote host .

Description

The rlogin service is running on the remote host . This service is vulnerable since data is passed between the rlogin client and server in cleartext . A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also,it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication .

Finally, rlogin is an easy way to turn file write access into full logins through the .rhosts or rhosts.equiv files .

Solution

Comment out the 'login' line in /etc/inetd.conf and restart the inetd process . Alternatively, disable this service and use SSH instead .

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/513/rlogin)

10245 (1) - rsh Service Detection

Synopsis

The rsh service is running on the remote host .

Description

The rsh service is running on the remote host . This service is vulnerable since data is passed between the rsh client and server in cleartext . A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also,it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication .

Finally, rsh is an easy way to turn file write access into full logins through the .rhosts or rhosts.equiv files .

Solution

Comment out the 'rsh' line in /etc/inetd.conf and restart the inetd process . Alternatively, disable this service and use SSH instead .

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/514/rsh)

19704 (1) - TWiki 'rev' Parameter Arbitrary Command Execution

Synopsis

The remote web server hosts a CGI application that is affected by an arbitrary command execution vulnerability.

Description

The version of TWiki running on the remote host allows an attacker to manipulate input to the 'rev' parameter in order to execute arbitrary shell commands on the remote host subject to the privileges of the web server user id.

Solution

Apply the appropriate hotfix referenced in the vendor advisory.

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/80/www)

36171 (1) - phpMyAdmin Setup Script Configuration Parameters Arbitrary P Code Injection (PMASA-2009-4)

Synopsis

The remote web server contains a PHP application that is affected by a code execution vulnerability .

Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user supplied input before using it to generate a config file for the application . This version is affected by the following vulnerabilities :

- The setup script inserts the unsanitized verbose server name into a C style comment during config file generation.

- An attacker can save arbitrary data to the generated config file by altering the value of the 'textconfig' parameter during a POST request to config php .

An unauthenticated remote attacker can exploit these issues to execute arbitrary PHP code .

Solution

Upgrade to phpMyAdmin 3.1.3.2. Alternatively, apply the patches referenced in the project's advisory .

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/80/www)

39469 (1) - CGI Generic Remote File Inclusion

Synopsis

Arbitrary code may be run on the remote server .

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings. By leveraging this issue , an attacker may be able to include a remote file from a remote server and execute arbitrary commands on the target host.

Solution

Restrict access to the vulnerable application . Contact the vendor for a patch or upgrade.

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/80/www)

42256 (1) - NFS Shares World Readable

Synopsis

The remote NFS server exports world readable shares .

Description

The remote NFS server is exporting one or more shares without restricting access (based on hostname , IP, or IP range).

Solution

Place the appropriate restrictions on all NFS shares .

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/2049/rpc-nfs)

59088 (1) - PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution

Synopsis

The remote web server contains a version of PHP that allows arbitrary code execution .

Description

The PHP installation on the remote web server contains a flaw that could allow a remote attacker to pass command-line arguments as part of a query string to the PHP CGI program.This could be abused to execute arbitrary code , reveal PHP source code , cause a system crash , etc.

Solution

If using Lotus Foundations , upgrade the Lotus Foundations operating system to version 1.2.2b or later.

Otherwise, upgrade to PHP 5.3.13 / 5.4.3 or later.

Risk Factor

High

Plugin Output

192.168.60.101 (tcp/80/www)

90509 (1) - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability .

Description

The version of Samba, a CIFS/SMB server for Linux and Unix , running on the remote host is affected by a flaw, known as Badlock , that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user , such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/445/cifs)

136769 (1) - ISC BIND Service Downgrade / Reflected DoS

Synopsis

The remote name server is affected by Service Downgrade / Reflected DoS vulnerabilities .

Description

According to its self reported version , the instance of ISC BIND 9 running on the remote name server is affected by performance downgrade and Reflected DoS vulnerabilities . This is due to BIND DNS not sufficiently limiting the number fetches which may be performed while processing a referral response.

An unauthenticated, remote attacker can exploit this to cause degrade the service of the recursive server or to use the affected server as a reflector in a reflection attack .

Solution

Upgrade to the ISC BIND version referenced in the vendor advisory.

Risk Factor

Medium

Plugin Output

192.168.60.101 (udp/53/dns)

15901 (2) - SSL Certificate Expiry

Synopsis

The remote server's SSL certificate has already expired .

Description

This plugin checks expiry dates of certificates associated with SSL - enabled services on the target and reports whether any have already expired .

Solution

Purchase or generate a new SSL certificate to replace the existing one .

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)

192.168.60.101 (tcp/5432/postgresql)

45411 (2) - SSL Certificate with Wrong Hostname

Synopsis

The SSL certificate for this service is for a different host.

Description

The 'commonName' (CN)attribute of the SSL certificate presented for this service is for a different machine.

Solution

Purchase or generate a proper SSL certificate for this service .

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)

192.168.60.101 (tcp/5432/postgresql)

51192 (2) - SSL Certificate Cannot Be Trusted

Synopsis

The SSL certificate for this service cannot be trusted .

Description

The server's X .509 certificate cannot be trusted .This situation can occur in three different ways, in which the chain of trust can be broken , as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority . This can occur either when the top of the chain is an unrecognized self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority .

- Second,the certificate chain may contain a certificate that is not valid at the time of the scan . This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third,the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer . Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production , any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server . This could make it easier to carry out man-in-the-middle attacks against the remote host .

Solution

Purchase or generate a proper SSL certificate for this service .

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)

192.168.60.101 (tcp/5432/postgresql)

57582 (2) - SSL Self-Signed Certificate

Synopsis

The SSL certificate chain for this service ends in an unrecognized self signed certificate .

Description

The X .509 certificate chain for this service is not signed by a recognized certificate authority . If the remote host is a public host in production , this nullifies the use of SSL as anyone could establish a man in the - middle attack against the remote host .

Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed,but is signed by an unrecognized certificate authority .

Solution

Purchase or generate a proper SSL certificate for this service .

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)

192.168.60.101 (tcp/5432/postgresql)

65821 (2) - SSL RC4 Cipher Suites Supported (Bar Mitzvah)

Synopsis

The remote service supports the use of the RC 4 cipher.

Description

The remote host supports the use of RC4 in one or more cipher suites.

The RC 4 cipher is flawed in its generation of a pseudo random stream of bytes so that a wide variety of small biases are introduced into the stream decreasing its randomness .

If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext .

Solution

Reconfigure the affected application , if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support.

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)
192.168.60.101 (tcp/5432/postgresql)

104743 (2) - TLS Version 1.0 Protocol Detection

Synopsis

The remote service encrypts traffic using an older version of TLS.

Description

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.

As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

PCI DSS v 3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

Solution

Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)
192.168.60.101 (tcp/5432/postgresql)

11213 (1) - HTTP TRACE / TRACK Methods Allowed

Synopsis

Debugging functions are enabled on the remote web server.

Description

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

Solution

Disable these HTTP methods. Refer to the plugin output for more information.

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/80/www)

11229 (1) - Web Server info.php / phpinfo.php Detection

Synopsis

The remote web server contains a PHP script that is prone to an information disclosure attack.

Description

Many PHP installation tutorials instruct the user to create a PHP file that calls the PHP function 'phpinfo'() for debugging purposes. Various PHP applications may also include such a file. By accessing such a file, a remote attacker can discover a large amount of information about the remote web server, including:

- The username of the user who installed PHP and if they are a SUDO user.

- The IP address of the host.

- The version of the operating system.

- The web server version.

- The root directory of the web server.

- Configuration information about the remote PHP installation.

Solution

Remove the affected file(s).

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/80/www)

11411 (1) - Backup Files Disclosure

Synopsis

It is possible to retrieve file backups from the remote web server.

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

26928 (1) - SSL Weak Cipher Suites Supported

nd

delete or protect those files that should not be accessible .

Synopsis

Risk Factor

The remote service supports the use of weak SSL ciphers .

Medium

Description

Plugin Output

The remote host supports the use of SSL ciphers that offer weak encryption .

192.168.60.101 (tcp/80/www)

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application , if possible to avoid the use of weak ciphers .

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)

31705 (1) - SSL Anonymous Cipher Suites Supported

Synopsis

The remote service supports the use of anonymous SSL ciphers .

Description

The remote host supports the use of anonymous SSL ciphers . While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates , it offers no way to verify the remote host's identity and renders the service vulnerable to a man in the-middle attack .

Note: This is considerably easier to exploit if the attacker is on the same physical network.

Solution

Reconfigure the affected application if possible to avoid use of weak ciphers .

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/25/smtp)

36083 (1) - phpMyAdmin file_path Parameter Vulnerabilities (PMASA-2009-1

Synopsis

The remote web server contains a PHP script that is affected by multiple issues.

Description

The version of phpMyAdmin installed on the remote host fails to sanitize user-supplied input to the 'file_path' parameter of the 'bs_disp_as_mime_type.php' script before using it to read a file and reporting it in dynamically-generated HTML. An unauthenticated, remote attacker may be able to leverage this issue to read arbitrary files, possibly from third-party hosts, or to inject arbitrary HTTP headers in responses sent to third-party users.

Note that the application is also reportedly affected by several other issues, although Nessus has not actually checked for them.

Solution

Upgrade to phpMyAdmin 3.1.3.1 or apply the patch referenced in the project's advisory.

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/80/www)

39466 (1) - CGI Generic XSS (quick test)

Synopsis

The remote web server is prone to cross-site scripting attacks.

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious

executed in a user's browser within the security context of the affected site.

These XSS are likely to be 'non persistent' or 'reflected'.

Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade to address any cross-site scripting vulnerabilities.

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/80/www)

39467 (1) - CGI Generic Path Traversal

Synopsis

Arbitrary files may be accessed or executed on the remote host .

Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local files inclusion vulnerabilities .

By leveraging this issue , an attacker may be able to read arbitrary files on the web server or execute commands.

Solution

Restrict access to the vulnerable application . Contact the vendor for a patch or upgrade to address path traversal flaws.

Risk Factor

Medium

Plugin Output

192.168.60.101（tcp/80/www）

78479 (2) - SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)

Synopsis

It is possible to obtain sensitive information from the remote host with SSL/TLS-enabled services.

Description

The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.

MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections.

As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service.

The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism Sites that cannot disable SSLv3 immediately should enable this mechanism.

This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability.

Solution

Disable SSLv3.

Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled.

Risk Factor

Medium

Plugin Output

192.168.60.101 (tcp/25/smtp)

192.168.60.101 (tcp/5432/postgresql)

10407 (1) - X Server Detection

Synopsis

An X11 server is listening on the remote host

Description

The remote host is running an X 11 server. X11 is a client ~~-~~server protocol that can be used to display graphical applications running on a given host on a remote client .

Since the X 11 traffic is not ciphered,it is possible for an attacker to eavesdrop on the connection .

Solution

Restrict access to this port . If the X11 client/server facility is not used,disable TCP support in X11 entirely (-nolisten tcp).

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/6000/x11)

26194 (1) - Web Server Transmits Cleartext Credentials

Synopsis

The remote web server might transmit credentials in cleartext .

Description

The remote web server contains several HTML form fields containing an input of type 'password' which transmit their information to a remote web server in cleartext .

An attacker eavesdropping the traffic between web browser and server may obtain logins and passwords of valid users .

Solution

Make sure that every sensitive form transmits content over HTTPS.

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/80/www)

42057 (1) - Web Server Allows Password Auto-Completion

Synopsis

The 'autocomplete' attribute is not disabled on password fields .

Description

The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off' .

While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point .

Solution

Add the attribute 'autocomplete =off' to these fields to prevent browsers from caching credentials .

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/80/www)

70658 (1) - SSH Server CBC Mode Ciphers Enabled

Synopsis

The SSH server is configured to use Cipher Block Chaining .

Description

The SSH server is configured to support Cipher Block Chaining (CBC) encryption. This may allow an attacker to recover the plaintext message from the ciphertext .

Note that this plugin only checks for the options of the SSH server and does not check for vulnerable software versions .

Solution

Contact the vendor or consult product documentation to disable CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption .

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/22/ssh)

71049 (1) - SSH Weak MAC Algorithms Enabled

Synopsis

The remote SSH server is configured to allow MD 5 and 96-bit MAC algorithms .

Description

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms , both of which are considered weak .

Note that this plugin only checks for the options of the SSH server , and it does not check for vulnerable software versions .

Solution

Contact the vendor or consult product documentation to disable MD 5 and 96-bit MAC algorithms .

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/22/ssh)

83738 (1) - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supporte (Logjam)

Synopsis

The remote host supports a set of weak ciphers .

Description

The remote host supports EXPORT_DHE cipher suites with keys less than or equal to 512 bits. Through cryptanalysis, a third party can find the shared secret in a short amount of time.

A man in the middle attacker may be able to downgrade the session to use EXPORT DHE_cipher suites. Thus, it is recommended to remove support for weak cipher suites.

See Also

https://weakdh.org/

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/25/smtp)

83875 (1) - SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)

Synopsis

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits.

Description

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

See Also

https://weakdh.org/

Solution

Reconfigure the service to use a unique Diffie Hellman moduli of 2048 bits or greater.

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/25/smtp)

153953 (1) - SSH Weak Key Exchange Algorithms Enabled

Synopsis

The remote SSH server is configured to allow weak key exchange algorithms.

Description

The remote SSH server is configured to allow key exchange algorithms which are considered weak.

This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)draft ietf curdle ssh kex sha 2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled This includes :

diffie-hellman-group-exchange-sha 1

diffie-hellman-group 1-sha1

gss-gex-sha 1-*

gss-group 1-sha1-*

gss-group 14-sha1-*

rsa1024-sha1

Note that this plugin only checks for the options of the SSH server , and it does not check for vulnerable software versions .

Solution

Contact the vendor or consult product documentation to disable the weak algorithms .

Risk Factor

Low

Plugin Output

192.168.60.101 (tcp/22/ssh)

Others non critical vulnerabilities

- 10281 (1) - Telnet Server Detection
- 10287 (1) - Traceroute Information
- 10342 (1) - VNC Software Detection
- 10397 (1) - Microsoft Windows SMB LanMan Pipe Server Listing Disclosure
- 10437 (1) - NFS Share Export List
- 10662 (1) - Web mirroring
- 10719 (1) - MySQL Server Detection
- 10785 (1) - Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
- 10881 (1) - SSH Protocol Versions Supported
- 11032 (1) - Web Server Directory Enumeration
- 11153 (1) - Service Detection (HELP Request)
- 11156 (1) - IRC Daemon Version Detection
- 11419 (1) - Web Server Office File Inventory
- 11424 (1) - WebDAV Detection
- 11819 (1) - TFTP Daemon Detection
- 11936 (1) - OS Identification
- 17219 (1) - phpMyAdmin Detection
- 17975 (1) - Service Detection (GET request)
- 18261 (1) - Apache Banner Linux Distribution Disclosure
- 19288 (1) - VNC Server Security Type Detection
- 19506 (1) - Nessus Scan Information
- 19941 (1) - TWiki Detection
- 24004 (1) - WebDAV Directory Enumeration
- 24260 (1) - HyperText Transfer Protocol (HTTP) Information
- 25220 (1) - TCP/IP Timestamps Supported
- 25240 (1) - Samba Server Detection
- 26024 (1) - PostgreSQL Server Detection
- 33817 (1) - CGI Generic Tests Load Estimation (all tests)
- 35371 (1) - DNS Server hostname.bind Map Hostname Disclosure