# META#2

Report generated by Nessus™ Sat, 26 Aug 2023 12:46:01 EDT

TABLE OF CONTENTS

## Vulnerabilities by Host

# 192.168.60.101

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 14 | 11 | 40 | 13 | 165 |

## Scan Information

Start time: Sat Aug 26 12:19:09 2023
End time: Sat Aug 26 12:46:01 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

References

| | |
|---|---|
| BID | 53388 |
| CVE | CVE-2012-1823 |
| CVE | CVE-2012-2311 |
| CVE | CVE-2012-2335 |
| CVE | CVE-2012-2336 |
| XREF | CERT:520827 |
| XREF | EDB-ID:29290 |
| XREF | EDB-ID:29316 |
| XREF | CISA-KNOWN-EXPLOITED:2022/04/15 |

Plugin Output

tcp/80/www

## 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Synopsis

There is a vulnerable AJP connector listening on the remote host.

Description

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

Solution

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

Risk Factor

High

References

| | |
|---|---|
| CVE | CVE-2020-1745 |
| CVE | CVE-2020-1938 |
| XREF | CISA-KNOWN-EXPLOITED:2022/03/17 |
| XREF | CEA-ID:CEA-2020-0021 |

Plugin Output

tcp/8009/ajp13

## 171340 - Apache Tomcat SEoL (<= 5.5.x)

Synopsis

An unsupported version of Apache Tomcat is installed on the remote host.

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

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

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

Risk Factor

Critical

Plugin Output

tcp/8180/www

## 51988 - 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

tcp/1524/wild_shell

## 32314 - 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

References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

Plugin Output

tcp/22/ssh

## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL ch

### 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

### References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

### Plugin Output

tcp/25/smtp


## 32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL ch

### 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

References

| | |
|---|---|
| BID | 29179 |
| CVE | CVE-2008-0166 |
| XREF | CWE:310 |

Plugin Output

tcp/5432/postgresql

## 11356 - 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

References

| | |
|---|---|
| CVE | CVE-1999-0170 |
| CVE | CVE-1999-0211 |
| CVE | CVE-1999-0554 |

Plugin Output

udp/2049/rpc-nfs

## 20007 - 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

tcp/25/smtp

## 20007 - 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

tcp/5432/postgresql

## 33850 - 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

### References

| | |
|---|---|
| XREF | IAVA:0001-A-0502 |
| XREF | IAVA:0001-A-0648 |

### Plugin Output

tcp/0

## 46882 - 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 MD5 / SHA1 checksums, and re-install it.

### Risk Factor

Critical

### References

| | |
|---|---|
| BID | 40820 |
| CVE | CVE-2010-2075 |

### Plugin Output

tcp/6667/irc

## 61708 - 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

tcp/5900/vnc

## 125855 - 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

### References

| | |
|---|---|
| BID | 108617 |
| CVE | CVE-2019-11768 |

### Plugin Output

tcp/80/www

## 39469 - 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

### References

| | |
|---|---|
| XREF | CWE:73 |
| XREF | CWE:78 |
| XREF | CWE:98 |
| XREF | CWE:434 |
| XREF | CWE:473 |
| XREF | CWE:632 |
| XREF | CWE:714 |
| XREF | CWE:727 |
| XREF | CWE:801 |
| XREF | CWE:928 |
| XREF | CWE:929 |

### Plugin Output

tcp/80/www

## 136769 - 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

### References

| | |
|---|---|
| CVE | CVE-2020-8616 |
| XREF | IAVA:2020-A-0217-S |

### Plugin Output

udp/53/dns

## 42256 - 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.

## 59088 - 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.

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

### References

| | |
|---|---|
| BID | 53388 |
| CVE | CVE-2012-1823 |
| CVE | CVE-2012-2311 |
| XREF | CERT:520827 |
| XREF | EDB-ID:18834 |
| XREF | CISA-KNOWN-EXPLOITED:2022/04/15 |

### Plugin Output

tcp/80/www

### Solution

## 42873 - 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

### References

| | |
|---|---|
| CVE | CVE-2016-2183 |

### Plugin Output

tcp/25/smtp

## 42873 - 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

### References

| | |
|---|---|
| CVE | CVE-2016-2183 |

### Plugin Output

tcp/5432/postgresql

## 90509 - 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

### References

| | |
|---|---|
| BID | 86002 |
| CVE | CVE-2016-2118 |
| XREF | CERT:813296 |

### Plugin Output

tcp/445/cifs

## 19704 - 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

### References

| | |
|---|---|
| BID | 14834 |
| CVE | CVE-2005-2877 |

### Plugin Output

tcp/80/www

## 36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP 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

### References

| | |
|---|---|
| BID | 34526 |
| CVE | CVE-2009-1285 |
| XREF | TRA:TRA-2009-02 |
| XREF | SECUNIA:34727 |
| XREF | CWE:94 |

### Plugin Output

tcp/80/www

## 10205 - 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

### References

| | |
|---|---|
| CVE | CVE-1999-0651 |

### Plugin Output

tcp/513/rlogin

## 10245 - 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

### References

| | |
|---|---|
| CVE | CVE-1999-0651 |

### Plugin Output

tcp/514/rsh

## 12085 - Apache Tomcat Default Files

### Synopsis

The remote web server contains default files.

### Description

The default error page, default index page, example JSPs and/or example servlets are installed on the remote Apache Tomcat server. These files should be removed as they may help an attacker uncover information about the remote Tomcat install or host itself.

### Solution

Delete the default index page and remove the example JSP and servlets. Follow the Tomcat or OWASP instructions to replace or modify the default error page.

### Risk Factor

Medium

### Plugin Output

tcp/8180/www

## 11411 - 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.

### Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

### Risk Factor

Medium

### Plugin Output

tcp/80/www

## 40984 - Browsable Web Directories

### Synopsis

Some directories on the remote web server are browsable.

### Description

Multiple Nessus plugins identified directories on the web server that are browsable.

### Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

### Risk Factor

Medium

### Plugin Output

tcp/80/www

## 44136 - CGI Generic Cookie Injection Scripting

### Synopsis

The remote web server is prone to cookie injection attacks.

### Description

The remote web server hosts at least one CGI script that fails to adequately sanitize request strings with malicious JavaScript.

By leveraging this issue, an attacker may be able to inject arbitrary cookies. Depending on the structure of the web application, it may be possible to launch a 'session fixation' attack using this mechanism.

Please note that :

- Nessus did not check if the session fixation attack is feasible.

- This is not the only vector of session fixation.

### Solution

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

### Risk Factor

Medium

### References

| | |
|---|---|
| XREF | CWE:472 |
| XREF | CWE:642 |
| XREF | CWE:715 |
| XREF | CWE:722 |

### Plugin Output

tcp/80/www

## 49067 - CGI Generic HTML Injections (quick test)

### Synopsis

The remote web server may be prone to HTML injections.

### Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings with malicious JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML to be executed in a user's browser within the security context of the affected site.

The remote web server may be vulnerable to IFRAME injections or cross-site scripting attacks :

- IFRAME injections allow 'virtual defacement' that might scare or anger gullible users. Such injections are sometimes implemented for 'phishing' attacks.

- XSS are extensively tested by four other scripts.

- Some applications (e.g. web forums) authorize a subset of HTML without any ill effect. In this case, ignore this warning.

### Solution

Either restrict access to the vulnerable application or contact the vendor for an update.

### Risk Factor

Medium

### References

| | |
|---|---|
| XREF | CWE:80 |
| XREF | CWE:86 |

### Plugin Output

tcp/80/www

## 42872 - CGI Generic Local File Inclusion (2nd pass)

### Synopsis

Arbitrary code may be run on this 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 local file and disclose its contents, or even execute arbitrary code on the remote host.

### Solution

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

### Risk Factor

Medium

### References

| | |
|---|---|
| XREF | CWE:73 |
| XREF | CWE:78 |
| XREF | CWE:98 |
| XREF | CWE:473 |
| XREF | CWE:632 |
| XREF | CWE:714 |
| XREF | CWE:727 |
| XREF | CWE:928 |
| XREF | CWE:929 |

### Plugin Output

192.168.60.101 tcp/80/www

## 39467 - 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

### References

| | |
|---|---|
| XREF | OWASP:OWASP-AZ-001 |
| XREF | CWE:21 |
| XREF | CWE:22 |
| XREF | CWE:632 |
| XREF | CWE:715 |
| XREF | CWE:723 |
| XREF | CWE:813 |
| XREF | CWE:928 |
| XREF | CWE:932 |

### Plugin Output

tcp/80/www

## 39466 - 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 JavaScript. By leveraging this issue, an attacker may be able to cause arbitrary HTML and script code to be 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

Medium

### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:80 |
| XREF | CWE:81 |
| XREF | CWE:83 |
| XREF | CWE:86 |
| XREF | CWE:116 |
| XREF | CWE:442 |
| XREF | CWE:692 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:751 |
| XREF | CWE:801 |
| XREF | CWE:811 |
| XREF | CWE:928 |
| XREF | CWE:931 |

### Plugin Output

tcp/80/www

## 11213 - 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

### References

| | |
|---|---|
| BID | 9506 |
| BID | 9561 |
| BID | 11604 |
| BID | 33374 |
| BID | 37995 |
| CVE | |
| CVE | |
| CVE | |
| XREF | CERT:288308 |
| XREF | CERT:867593 |
| XREF | CWE:16 |
| XREF | CWE:200 |

### Plugin Output

tcp/80/www

## 139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

### Synopsis

The remote name server is affected by a denial of service vulnerability.

### Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### Solution

## 139915 - ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

### Synopsis

The remote name server is affected by a denial of service vulnerability.

### Description

According to its self-reported version number, the installation of ISC BIND running on the remote name server is version 9.x prior to 9.11.22, 9.12.x prior to 9.16.6 or 9.17.x prior to 9.17.4. It is, therefore, affected by a denial of service (DoS) vulnerability due to an assertion failure when attempting to verify a truncated response to a TSIG-signed request. An authenticated, remote attacker can exploit this issue by sending a truncated response to a TSIG-signed request to trigger an assertion failure, causing the server to exit.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### Solution

Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.

### Risk Factor

Medium

### References

| | |
|---|---|
| CVE | CVE-2020-8622 |
| XREF | IAVA:2020-A-0385-S |

### Plugin Output

udp/53/dns

## 136808 - ISC BIND Denial of Service

## 136808 - ISC BIND Denial of Service

### Synopsis

The remote name server is affected by an assertion failure vulnerability.

### Description

A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

### Solution

Upgrade to the patched release most closely related to your current version of BIND.

### Risk Factor

Medium

### References

| | |
|---|---|
| CVE | CVE-2020-8617 |
| XREF | IAVA:2020-A-0217-S |

### Plugin Output

udp/53/dns

## 46803 - PHP expose_php Information Disclosure

### Synopsis

The configuration of PHP on the remote host allows disclosure of sensitive information.

### Description

The PHP install on the remote server is configured in a way that allows disclosure of potentially sensitive information to an attacker through a special URL. Such a URL triggers an Easter egg built into PHP itself.

Other such Easter eggs likely exist, but Nessus has not checked for them.

### Solution

In the PHP configuration file, php.ini, set the value for 'expose_php' to 'Off' to disable this behavior. Restart the web server daemon to put this change into effect.

### Risk Factor

Medium

Plugin Output

tcp/80/www

## 57608 - SMB Signing not required

Synopsis

Signing is not required on the remote SMB server.

Description

conduct man-in-the-middle attacks against the SMB server.
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

Risk Factor

Medium

Plugin Output

tcp/445/cifs

## 52611 - SMTP Service STARTTLS Plaintext Command Injection

Synopsis

The remote mail service allows plaintext command injection while negotiating an encrypted communications channel.

Description

The remote SMTP service contains a software flaw in its STARTTLS implementation that could allow a remote, unauthenticated attacker to inject commands during the plaintext protocol phase that will be executed during the ciphertext protocol phase.

Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.

Solution

Contact the vendor to see if an update is available.

Risk Factor

Medium

References

| | |
|---|---|
| BID | 46767 |
| CVE | CVE-2011-0411 |
| CVE | CVE-2011-1430 |
| CVE | CVE-2011-1431 |
| CVE | CVE-2011-1432 |
| CVE | CVE-2011-1506 |
| CVE | CVE-2011-2165 |
| XREF | CERT:555316 |

Plugin Output

tcp/25/smtp

## 90317 - SSH Weak Algorithms Supported

Synopsis

The remote SSH server is configured to allow weak encryption algorithms or no algorithm at all.

Description

Nessus has detected that the remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Solution

Contact the vendor or consult product documentation to remove the weak ciphers.

Risk Factor

Medium

Plugin Output

tcp/22/ssh

## 31705 - 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

### References

| | |
|---|---|
| BID | 28482 |
| CVE | CVE-2007-1858 |

### Plugin Output

tcp/25/smtp

## 51192 - 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

tcp/25/smtp

# 51192 - 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

tcp/5432/postgresql

## 15901 - 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

tcp/25/smtp

## 15901 - 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

tcp/5432/postgresql

## 45411 - 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

tcp/25/smtp

## 45411 - 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

tcp/5432/postgresql

## 89058 - SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)

### Synopsis

The remote host may be affected by a vulnerability that allows a remote attacker to potentially decrypt captured TLS traffic.

### Description

The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key.

### Solution

Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections.

### Risk Factor

Medium

### References

| | |
|---|---|
| BID | 83733 |
| CVE | CVE-2016-0800 |
| XREF | CERT:583776 |

### Plugin Output

tcp/25/smtp

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

### Synopsis

The remote service supports the use of the RC4 cipher.

### Description

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

The RC4 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

References

| | |
|---|---|
| BID | 58796 |
| BID | 73684 |
| CVE | CVE-2013-2566 |
| CVE | CVE-2015-2808 |

Plugin Output

tcp/25/smtp

## 57582 - 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

tcp/5432/postgresql

## 26928 - SSL Weak Cipher Suites Supported

### Synopsis

The remote service supports the use of weak SSL ciphers.

### Description

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

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

### References

| | |
|---|---|
| XREF | CWE:326 |
| XREF | CWE:327 |
| XREF | CWE:720 |
| XREF | CWE:753 |
| XREF | CWE:803 |
| XREF | CWE:928 |
| XREF | CWE:934 |

### Plugin Output

tcp/25/smtp

## 81606 - SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

### Synopsis

The remote host supports a set of weak ciphers.

### Description

The remote host supports EXPORT_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time.

A man-in-the middle attacker may be able to downgrade the session to use EXPORT_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites.

### Solution

Reconfigure the service to remove support for EXPORT_RSA cipher suites.

### Risk Factor

Medium

### References

| | |
|---|---|
| BID | 71936 |
| CVE | CVE-2015-0204 |
| XREF | CERT:243585 |

### Plugin Output

tcp/25/smtp

## 104743 - 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 v3.2 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

### References

XREF CWE:327

### Plugin Output

tcp/25/smtp

## 104743 - 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 v3.2 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

References

XREF CWE:327

Plugin Output

tcp/5432/postgresql

## 35806 - Tomcat Sample App cal2.jsp 'time' Parameter XSS

### Synopsis

The remote web server contains a JSP application that is affected by a cross-site scripting vulnerability.

### Description

The remote web server includes an example JSP application, 'cal2.jsp', that fails to sanitize user-supplied input before using it to generate dynamic content. An unauthenticated, remote attacker can exploit this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site.

Solution

Upgrade to Apache Tomcat version 4.1.40 / 5.5.28 / 6.0.20.

Alternatively, apply the appropriate patch referenced in the vendor advisory or undeploy the Tomcat examples web application.

Risk Factor

Medium

References

| | |
|---|---|
| CVE | CVE-2009-0781 |
| XREF | CWE:79 |

Plugin Output

tcp/8180/www

## 42263 - Unencrypted Telnet Server

Synopsis

The remote Telnet server transmits traffic in cleartext.

Description

The remote host is running a Telnet server over an unencrypted channel.

Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.

SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.

Solution

Disable the Telnet service and use SSH instead.

Risk Factor

Medium

Plugin Output

tcp/23/telnet

## 57640 - Web Application Information Disclosure

### Synopsis

The remote web application discloses path information.

### Description

At least one web application hosted on the remote web server discloses the physical path to its directories when a malformed request is sent to it.

Leaking this kind of information may help an attacker fine-tune attacks against the application and its backend.

### Solution

Filter error messages containing path information.

### Risk Factor

Medium

### Plugin Output

tcp/80/www

## 85582 - Web Application Potentially Vulnerable to Clickjacking

### Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

### Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

## Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

## Risk Factor

Medium

## References

XREF CWE:693

## Plugin Output

tcp/80/www

## 85582 - Web Application Potentially Vulnerable to Clickjacking

### Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

### Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

### Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.

This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

### Risk Factor

Medium

### References

XREF CWE:693

### Plugin Output

tcp/8180/www

References

XREF CWE:693

Plugin Output

tcp/8180/www

## 11229 - 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.

## 11229 - 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

tcp/80/www

## 51425 - phpMyAdmin error.php BBcode Tag XSS (PMASA-2010-9)

### Synopsis

The remote web server hosts a PHP script that is prone to a cross- site scripting attack.

### Description

The version of phpMyAdmin fails to validate BBcode tags in user input to the 'error' parameter of the 'error.php' script before using it to generate dynamic HTML.

An attacker may be able to leverage this issue to inject arbitrary HTML or script code into a user's browser to be executed within the security context of the affected site. For example, this could be used to cause a page with arbitrary text and a link to an external site to be displayed.

### Solution

Upgrade to phpMyAdmin 3.4.0-beta1 or later.

### Risk Factor

Medium

References

| | |
|---|---|
| BID | 45633 |
| CVE | CVE-2010-4480 |
| XREF | EDB-ID:15699 |
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

Plugin Output

tcp/80/www

## 36083 - 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

Medium

### References

| | |
|---|---|
| BID | 34253 |
| XREF | SECUNIA:34468 |

### Plugin Output

tcp/80/www

## 49142 - phpMyAdmin setup.php Verbose Server Name XSS (PMASA-2010-7)

### Synopsis

The remote web server contains a PHP application that has a cross- site scripting vulnerability.

### Description

The setup script included with the version of phpMyAdmin installed on the remote host does not properly sanitize user-supplied input to the 'verbose server name' field.

A remote attacker could exploit this by tricking a user into executing arbitrary script code.

### Solution

Upgrade to phpMyAdmin 3.3.7 or later.

### Risk Factor

Medium

### References

| | |
|---|---|
| CVE | CVE-2010-3263 |
| XREF | TRA:TRA-2010-02 |
| XREF | CWE:20 |
| XREF | CWE:74 |
| XREF | CWE:79 |
| XREF | CWE:442 |
| XREF | CWE:629 |
| XREF | CWE:711 |
| XREF | CWE:712 |
| XREF | CWE:722 |
| XREF | CWE:725 |
| XREF | CWE:750 |
| XREF | CWE:751 |
| XREF | CWE:800 |
| XREF | CWE:801 |
| XREF | CWE:809 |
| XREF | CWE:811 |
| XREF | CWE:864 |
| XREF | CWE:900 |
| XREF | CWE:928 |
| XREF | CWE:931 |
| XREF | CWE:990 |

### Plugin Output

tcp/80/www

## 70658 - 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

### References

| | |
|---|---|
| BID | 32319 |
| CVE | CVE-2008-5161 |
| XREF | CERT:958563 |
| XREF | CWE:200 |

### Plugin Output

tcp/22/ssh

## 153953 - 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-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:

diffie-hellman-group-exchange-sha1

diffie-hellman-group1-sha1

gss-gex-sha1-*

gss-group1-sha1-*

gss-group14-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

tcp/22/ssh

## 71049 - SSH Weak MAC Algorithms Enabled

### Synopsis

The remote SSH server is configured to allow MD5 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 MD5 and 96-bit MAC algorithms.

### Risk Factor

Low

### Plugin Output

tcp/22/ssh

## 83875 - 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.

Solution

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

Risk Factor

Low

References

| | |
|---|---|
| BID | 74733 |
| CVE | CVE-2015-4000 |
| XREF | CEA-ID:CEA-2021-0004 |

Plugin Output

tcp/25/smtp

## 83738 - SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (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.

Solution

Reconfigure the service to remove support for EXPORT_DHE cipher suites.

Risk Factor

Low

References

| | |
|---|---|
| BID | 74733 |
| CVE | CVE-2015-4000 |
| XREF | CEA-ID:CEA-2021-0004 |

Plugin Output

tcp/25/smtp

## 78479 - 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.

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

tcp/80/www

## 42057 - 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.

### References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:523 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

Plugin Output

tcp/80/www

## 26194 - 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

References

| | |
|---|---|
| XREF | CWE:522 |
| XREF | CWE:523 |
| XREF | CWE:718 |
| XREF | CWE:724 |
| XREF | CWE:928 |
| XREF | CWE:930 |

Plugin Output

tcp/8180/www

## 34850 - Web Server Uses Basic Authentication Without HTTPS

Synopsis

The remote web server seems to transmit credentials in cleartext.

Description

The remote web server contains web pages that are protected by 'Basic' authentication over cleartext.

An attacker eavesdropping the traffic might obtain logins and passwords of valid users.

Solution

Make sure that HTTP authentication is transmitted over HTTPS.

Risk Factor

Low

References

| | |
|---|---|
| XREF | CWE:319 |
| XREF | CWE:928 |
| XREF | CWE:930 |
| XREF | CWE:934 |

Plugin Output

tcp/8180/www

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 10223 | RPC portmapper Service Detection |
| INFO | N/A | - | 21186 | AJP Connector Detection |
| INFO | N/A | - | 18261 | Apache Banner Linux Distribution Disclosure |
| INFO | N/A | - | 48204 | Apache HTTP Server Version |
| INFO | N/A | - | 39446 | Apache Tomcat Detection |
| INFO | N/A | - | 39519 | Backported Security Patch Detection (FTP) |
| INFO | N/A | - | 84574 | Backported Security Patch Detection (PHP) |
| INFO | N/A | - | 39520 | Backported Security Patch Detection (SSH) |
| INFO | N/A | - | 39521 | Backported Security Patch Detection (WWW) |
| INFO | N/A | - | 47830 | CGI Generic Injectable Parameter |
| INFO | N/A | - | 33817 | CGI Generic Tests Load Estimation (all tests) |
| INFO | N/A | - | 45590 | Common Platform Enumeration (CPE) |
| INFO | N/A | - | 10028 | DNS Server BIND version Directive Remote Version Detection |
| INFO | N/A | - | 11002 | DNS Server Detection |
| INFO | N/A | - | 35371 | DNS Server hostname.bind Map Hostname Disclosure |
| INFO | N/A | - | 54615 | Device Type |
| INFO | N/A | - | 49704 | External URLs |
| INFO | N/A | - | 10092 | FTP Server Detection |
| INFO | N/A | - | 43111 | HTTP Methods Allowed (per directory) |
| INFO | N/A | - | 10107 | HTTP Server Type and Version |
| INFO | N/A | - | 24260 | HyperText Transfer Protocol (HTTP) Information |
| INFO | N/A | - | 11156 | IRC Daemon Version Detection |
| INFO | N/A | - | 10397 | Microsoft Windows SMB LanMan Pipe Server Listing Disclosure |
| INFO | N/A | - | 10785 | Microsoft Windows SMB NativeLanManager Remote System Information Disclosure |
| INFO | N/A | - | 11011 | Microsoft Windows SMB Service Detection |

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 100871 | Microsoft Windows SMB Versions Supported (remote check) |
| INFO | N/A | - | 106716 | Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check) |
| INFO | N/A | - | 50344 | Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header |
| INFO | N/A | - | 50345 | Missing or Permissive X-Frame-Options HTTP Response Header |
| INFO | N/A | - | 10719 | MySQL Server Detection |
| INFO | N/A | - | 10437 | NFS Share Export List |
| INFO | N/A | - | 11219 | Nessus SYN scanner |
| INFO | N/A | - | 19506 | Nessus Scan Information |
| INFO | N/A | - | 11936 | OS Identification |
| INFO | N/A | - | 117886 | OS Security Patch Assessment Not Available |
| INFO | N/A | - | 50845 | OpenSSL Detection |
| INFO | N/A | - | 48243 | PHP Version Detection |
| INFO | N/A | - | 66334 | Patch Report |
| INFO | N/A | - | 118224 | PostgreSQL STARTTLS Support |
| INFO | N/A | - | 26024 | PostgreSQL Server Detection |
| INFO | N/A | - | 40665 | Protected Web Page Detection |
| INFO | N/A | - | 22227 | RMI Registry Detection |
| INFO | N/A | - | 11111 | RPC Services Enumeration |
| INFO | N/A | - | 53335 | RPC portmapper (TCP) |
| INFO | N/A | - | 10263 | SMTP Server Detection |
| INFO | N/A | - | 42088 | SMTP Service STARTTLS Command Support |
| INFO | N/A | - | 70657 | SSH Algorithms and Languages Supported |
| INFO | N/A | - | 149334 | SSH Password Authentication Accepted |
| INFO | N/A | - | 10881 | SSH Protocol Versions Supported |

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 153588 | SSH SHA-1 HMAC Algorithms Enabled |
| INFO | N/A | - | 10267 | SSH Server Type and Version Information |
| INFO | N/A | - | 56984 | SSL / TLS Versions Supported |
| INFO | N/A | - | 45410 | SSL Certificate 'commonName' Mismatch |
| INFO | N/A | - | 10863 | SSL Certificate Information |
| INFO | N/A | - | 70544 | SSL Cipher Block Chaining Cipher Suites Supported |
| INFO | N/A | - | 21643 | SSL Cipher Suites Supported |
| INFO | N/A | - | 62563 | SSL Compression Methods Supported |
| INFO | N/A | - | 57041 | SSL Perfect Forward Secrecy Cipher Suites Supported |
| INFO | N/A | - | 51891 | SSL Session Resume Supported |
| INFO | N/A | - | 156899 | SSL/TLS Recommended Cipher Suites |
| INFO | N/A | - | 25240 | Samba Server Detection |
| INFO | N/A | - | 104887 | Samba Version |
| INFO | N/A | - | 96982 | Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check) |
| INFO | N/A | - | 22964 | Service Detection |
| INFO | N/A | - | 17975 | Service Detection (GET request) |
| INFO | N/A | - | 11153 | Service Detection (HELP Request) |
| INFO | N/A | - | 25220 | TCP/IP Timestamps Supported |
| INFO | N/A | - | 11819 | TFTP Daemon Detection |
| INFO | N/A | - | 19941 | TWiki Detection |
| INFO | N/A | - | 110723 | Target Credential Status by Authentication Protocol - No Credentials Provided |
| INFO | N/A | - | 10281 | Telnet Server Detection |
| INFO | N/A | - | 10287 | Traceroute Information |
| INFO | N/A | - | 11154 | Unknown Service Detection: Banner Retrieval |

| | | | | |
|---|---|---|---|---|
| INFO | N/A | - | 19288 | VNC Server Security Type Detection |
| INFO | N/A | - | 65792 | VNC Server Unencrypted Communication Detection |
| INFO | N/A | - | 10342 | VNC Software Detection |
| INFO | N/A | - | 135860 | WMI Not Available |
| INFO | N/A | - | 100669 | Web Application Cookies Are Expired |
| INFO | N/A | - | 85601 | Web Application Cookies Not Marked HttpOnly |
| INFO | N/A | - | 85602 | Web Application Cookies Not Marked Secure |
| INFO | N/A | - | 40773 | Web Application Potentially Sensitive CGI Parameter Detection |
| INFO | N/A | - | 91815 | Web Application Sitemap |
| INFO | N/A | - | 20108 | Web Server / Application favicon.ico Vendor Fingerprinting |
| INFO | N/A | - | 11032 | Web Server Directory Enumeration |
| INFO | N/A | - | 49705 | Web Server Harvested Email Addresses |
| INFO | N/A | - | 11419 | Web Server Office File Inventory |
| INFO | N/A | - | 11422 | Web Server Unconfigured - Default Install Page Present |
| INFO | N/A | - | 10662 | Web mirroring |
| INFO | N/A | - | 11424 | WebDAV Detection |
| INFO | N/A | - | 24004 | WebDAV Directory Enumeration |
| INFO | N/A | - | 10150 | Windows NetBIOS / SMB Remote Host Information Disclosure |
| INFO | N/A | - | 17219 | phpMyAdmin Detection |
| INFO | N/A | - | 52703 | vsftpd Detection |