OpenVas Vulnerability Report

Table of Contents

Summary

Scan started: **Fri Jun 27 19:47:29 2025 IST**
Scan ended: Fri Jun 27 21:49:37 2025 IST

18	36	3
HIGH	MEDIUM	LOW

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.109	Jun 27, 19:47	Jun 27, 21:49	18	36	3	0
Total: 1			18	36	3	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	DistCC Remote Code Execution Vulnerability	9.3	1
High	MySQL / MariaDB weak password	9.0	1
High	PostgreSQL weak password	9.0	1
High	VNC Brute Force Login	9.0	1
High	rlogin Passwordless / Unencrypted Cleartext Login	7.5	1
High	phpinfo() output Reporting	7.5	1
High	Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	7.5	1
High	PHP-CGI-based setups vulnerability when parsing query string parameters from ph...	7.5	1
High	vsftpd Compromised Source Packages Backdoor Vulnerability	7.5	2
High	Check for Backdoor in UnrealIRCd	7.5	1
High	Test HTTP dangerous methods	7.5	1
High	SSH Brute Force Logins With Default Credentials Reporting	7.5	1
Medium	UnrealIRCd Authentication Spoofing Vulnerability	6.8	1
Medium	TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8	1
Medium	SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	6.8	1
Medium	Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection ...	6.8	1
Medium	Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability	6.5	1
Medium	Anonymous FTP Login Reporting	6.4	1
Medium	TWiki Cross-Site Request Forgery Vulnerability	6.0	1
Medium	Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check)	6.0	1
Medium	HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8	1

Medium	Check if Mailserver answer to VRFY and EXPN requests	5.0	1
Medium	SSL/TLS: Certificate Expired	5.0	2
Medium	TWiki < 6.1.0 XSS Vulnerability	5.0	1
Medium	/doc directory browsable	5.0	1
Medium	Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability	5.0	1
Medium	Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability	5.0	1
Medium	awiki Multiple Local File Include Vulnerabilities	5.0	1
Medium	VNC Server Unencrypted Data Transmission	4.8	1
Medium	Telnet Unencrypted Cleartext Login	4.8	1
Medium	FTP Unencrypted Cleartext Login	4.8	2
Medium	Cleartext Transmission of Sensitive Information via HTTP	4.8	1
Medium	SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ...	4.3	2
Medium	SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	4.3	2
Medium	SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	4.3	1
Medium	SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)	4.3	1
Medium	SSL/TLS: Report Weak Cipher Suites	4.3	1
Medium	SSH Weak Encryption Algorithms Supported	4.3	1
Medium	phpMyAdmin 'error.php' Cross Site Scripting Vulnerability	4.3	1
Medium	Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3	1
Medium	SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0	2
Medium	SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili...	4.0	2
Low	Tiki Wiki CMS Groupware XSS Vulnerability	3.5	1
Low	TCP timestamps	2.6	1
Low	SSH Weak MAC Algorithms Supported	2.6	1
High	TWiki XSS and Command Execution Vulnerabilities	10.0	1
High	OS End Of Life Detection	10.0	1
High	Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0	1
High	Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil...	10.0	1
High	Possible Backdoor: Ingreslock	10.0	1

Results by Host

Host 192.168.1.109

Host scan started: Fri Jun 13 19:47:44 2025 IST

Port Summary for Host 192.168.1.109

Service (Port)	Severity
22/tcp	High
1524/tcp	High
3306/tcp	High
3632/tcp	High
5900/tcp	High
6200/tcp	High
23/tcp	Medium
80/tcp	High
2121/tcp	Medium
general/tcp	High
6667/tcp	High
21/tcp	High
8787/tcp	High
1099/tcp	High
25/tcp	Medium
5432/tcp	High
513/tcp	High
445/tcp	Medium

Security Issues for Host 192.168.1.109

High (CVSS: 10.0) 80/tcp
NVT: TWiki XSS and Command Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800320)

Product detection result: cpe:/a:twiki:twiki:01.Feb.2003 by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary

The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.

Vulnerability Detection Result

Installed version: 01.Feb.2003
Fixed version: 4.2.4

Impact

Successful exploitation could allow execution of arbitrary script code or commands. This could let attackers steal cookie-based authentication credentials or compromise the affected application.

Solution

Solution type: VendorFix

Upgrade to version 4.2.4 or later.

Affected Software/OS

TWiki, TWiki version prior to 4.2.4.

Vulnerability Insight

The flaws are due to,

- %URLPARAM{}% variable is not properly sanitized which lets attackers conduct cross-site scripting attack.

- %SEARCH{}% variable is not properly sanitised before being used in an eval() call which lets the attackers execute perl code through eval injection attack.

Vulnerability Detection Method

Details: TWiki XSS and Command Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.800320)

Version used: $Revision: 12952 $

Product Detection Result

Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

References

CVE: CVE-2008-5304, CVE-2008-5305
BID: 32668, 32669
Other: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304
http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305

High (CVSS: 10.0) general/tcp
NVT: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Product detection result: cpe:/o:canonical:ubuntu_linux:8.04 by OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

Summary

OS End Of Life Detection

The Operating System on the remote host has reached the end of life and should not be used anymore.

Vulnerability Detection Result

The "Ubuntu" Operating System on the remote host has reached the end of life.

CPE: cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP: 8.04
EOL date: 2013-05-09
EOL info: https://wiki.ubuntu.com/Releases

Solution

Solution type: Mitigation

Vulnerability Detection Method

Details: OS End Of Life Detection (OID: 1.3.6.1.4.1.25623.1.0.103674)

Version used: $Revision: 8927 $

Product Detection Result

Product: cpe:/o:canonical:ubuntu_linux:8.04
Method: OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

High (CVSS: 10.0) 8787/tcp
NVT: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.108010)

Summary

Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

Vulnerability Detection Result

The service is running in $SAFE >= 1 mode. However it is still possible to run arbitrary syscall commands on the remote host. Sending an invalid syscall the service returned the following response:

Flo:Errno::ENOSYS:bt["3/usr/lib/ruby/1.8/drb/drb.rb:1555:in `syscall'"0/usr/lib/ruby/1.8/drb/drb.rb:1555:in `send'"4/usr/lib/ruby/1.8/drb/drb.rb:1555:in `__send__'"A/usr/lib/ruby/1.8/drb/drb.rb:1555:in `perform_without_block'"3/usr/lib/ruby/1.8/drb/drb.rb:1515:in `perform'"5/usr/lib/ruby/1.8/drb/drb.rb:1589:in `main_loop'"0/usr/lib/ruby/1.8/drb/drb.rb:1585:in `loop'"5/usr/lib/ruby/1.8/drb/drb.rb:1585:in `main_loop'"1/usr/lib/ruby/1.8/drb/drb.rb:1581:in `start'"5/usr/lib/ruby/1.8/drb/drb.rb:1581:in `main_loop'"//usr/lib/ruby/1.8/drb/drb.rb:1430:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/drb/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//usr/lib/ruby/1.8/drb/drb.rb:1627:in `new'"9/usr/lib/ruby/1.8/drb/drb.rb:1627:in `start_service'"%/usr/sbin/druby_timeserver.rb:12:errnoi+:mesg"Function not implemented

Impact

By default, Distributed Ruby does not impose restrictions on allowed hosts or set the $SAFE environment variable to prevent privileged activities. If other controls are not in place, especially if the Distributed Ruby process runs with elevated privileges, an attacker could execute arbitrary system commands or Ruby scripts on the Distributed Ruby server. An attacker may need to know only the URI of the listening Distributed Ruby server to submit Ruby commands.

Solution

Solution type: Mitigation

Administrators of environments that rely on Distributed Ruby should ensure that appropriate controls are in place. Code-level controls may include:

- Implementing taint on untrusted input

- Setting $SAFE levels appropriately (>=2 is recommended if untrusted hosts are allowed to submit Ruby commands, and >=3 may be appropriate)

- Including drb/acl.rb to set ACLEntry to restrict access to trusted hosts

Vulnerability Detection Method

Send a crafted command to the service and check for a remote command execution via the instance_eval or syscall requests.

Details: Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.108010)

Version used: $Revision: 12338 $

References

BID:	47071
Other:	https://tools.cisco.com/security/center/viewAlert.x?alertId=22750
	http://www.securityfocus.com/bid/47071
	http://blog.recurity-labs.com/archives/2011/05/12/druby_for_penetration_testers/
	http://www.ruby-doc.org/stdlib-1.9.3/libdoc/drb/rdoc/DRb.html

High (CVSS: 10.0) 1099/tcp
NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil... (OID: 1.3.6.1.4.1.25623.1.0.140051)

Summary

Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Solution type: Workaround

Disable class-loading.

Vulnerability Insight

The vulnerability exists because of an incorrect default configuration of the Remote Method Invocation (RMI) Server in the affected software. An unauthenticated, remote attacker could exploit the vulnerability by transmitting crafted packets to the affected software. When the packets are processed, the attacker could execute arbitrary code on the system with elevated privileges.

Vulnerability Detection Method

Check if the target tries to load a Java class via a remote HTTP URL.

Details: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerabil... (OID: 1.3.6.1.4.1.25623.1.0.140051)

Version used: $Revision: 11922 $

References

Other: https://tools.cisco.com/security/center/viewAlert.x?alertId=23665

High (CVSS: 10.0) 1524/tcp
NVT: Possible Backdoor: Ingreslock (OID: 1.3.6.1.4.1.25623.1.0.103549)

Summary

A backdoor is installed on the remote host

Vulnerability Detection Result

The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution

Solution type: Workaround

Vulnerability Detection Method

Details: Possible Backdoor: Ingreslock (OID: 1.3.6.1.4.1.25623.1.0.103549)

Version used: $Revision: 11327 $

High (CVSS: 9.3) 3632/tcp
NVT: DistCC Remote Code Execution Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103553)

Summary

DistCC 2.x, as used in XCode 1.5 and others, when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Vulnerability Detection Result

It was possible to execute the "id" command.

Result: uid=1(daemon) gid=1(daemon)

Impact

DistCC by default trusts its clients completely that in turn could allow a malicious client to execute arbitrary commands on the server.

Solution

Solution type: VendorFix

Vendor updates are available. Please see the references for more information.

For more information about DistCC's security see the references.

Vulnerability Detection Method

Details: DistCC Remote Code Execution Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103553)

Version used: $Revision: 12032 $

References

CVE: CVE-2004-2687

Other: https://distcc.github.io/security.html

https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80/archives/bugtraq/2005-03/0183.html

High (CVSS: 9.0) 3306/tcp
NVT: MySQL / MariaDB weak password (OID: 1.3.6.1.4.1.25623.1.0.103551)

Product detection result: cpe:/a:mysql:mysql:5.0.51a by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

Summary

It was possible to login into the remote MySQL as root using weak credentials.

Vulnerability Detection Result

It was possible to login as root with an empty password.

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: MySQL / MariaDB weak password (OID: 1.3.6.1.4.1.25623.1.0.103551)

Version used: $Revision: 12175 $

Product Detection Result

Product: cpe:/a:mysql:mysql:5.0.51a
Method: MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

High (CVSS: 9.0) 5432/tcp
NVT: PostgreSQL weak password (OID: 1.3.6.1.4.1.25623.1.0.103552)

Product detection result: cpe:/a:postgresql:postgresql:8.3.1 by PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Summary

It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Vulnerability Detection Result

It was possible to login as user postgres with password "postgres".

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Details: PostgreSQL weak password (OID: 1.3.6.1.4.1.25623.1.0.103552)

Version used: $Revision: 10312 $

Product Detection Result

Product: cpe:/a:postgresql:postgresql:8.3.1
Method: PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

High (CVSS: 9.0) 5900/tcp
NVT: VNC Brute Force Login (OID: 1.3.6.1.4.1.25623.1.0.106056)

Summary

Try to log in with given passwords via VNC protocol.

Vulnerability Detection Result

It was possible to connect to the VNC server with the password: password

Solution

Solution type: Mitigation

Change the password to something hard to guess or enable password protection at all.

Vulnerability Insight

This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.

Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.

Note as well that passwords can be max. 8 characters long.

Vulnerability Detection Method

Details: VNC Brute Force Login (OID: 1.3.6.1.4.1.25623.1.0.106056)

Version used: $Revision: 13328 $

High (CVSS: 7.5) 513/tcp
NVT: rlogin Passwordless / Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.901202)

Summary

This remote host is running a rlogin service.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Solution type: Mitigation

Disable the rlogin service and use alternatives like SSH instead.

Vulnerability Insight

rlogin has several serious security problems,

- all information, including passwords, is transmitted unencrypted.

- .rlogin (or .rhosts) file is easy to misuse (potentially allowing anyone to login without a password)

Vulnerability Detection Method

Details: rlogin Passwordless / Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.901202)

Version used: $Revision: 13541 $

References

Other: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0651
http://en.wikipedia.org/wiki/Rlogin
http://www.ietf.org/rfc/rfc1282.txt

High (CVSS: 7.5) 80/tcp
NVT: phpinfo() output Reporting (OID: 1.3.6.1.4.1.25623.1.0.11229)

Summary

Many PHP installation tutorials instruct the user to create a file called phpinfo.php or similar containing the phpinfo() statement. Such a file is often left back in the webserver directory.

Vulnerability Detection Result

The following files are calling the function phpinfo() which disclose potentially sensitive information:

http://192.168.1.109/mutillidae/phpinfo.php
http://192.168.1.109/phpinfo.php

Impact

Some of the information that can be gathered from this file includes:

The username of the user running the PHP process, if it is a sudo user, the IP address of the host, the web server version, the system version (Unix, Linux, Windows, ...), and the root directory of the web server.

Solution

Solution type: Workaround

Delete the listed files or restrict access to them.

Vulnerability Detection Method

Details: phpinfo() output Reporting (OID: 1.3.6.1.4.1.25623.1.0.11229)

Version used: $Revision: 11992 $

High (CVSS: 7.5) 80/tcp
NVT: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100537)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary

Tiki Wiki CMS Groupware is prone to multiple unspecified vulnerabilities, including:

- An unspecified SQL-injection vulnerability - An unspecified authentication-bypass vulnerability - An unspecified vulnerability

Vulnerability Detection Result

Installed version: 1.9.5
Fixed version: 4.2

Impact

Exploiting these issues could allow an attacker to compromise the application, access or modify data, exploit latent vulnerabilities in the underlying database, and gain unauthorized access to the affected application. Other attacks are also possible.

Solution

Solution type: VendorFix

The vendor has released an advisory and fixes. Please see the references for details.

Affected Software/OS

Versions prior to Tiki Wiki CMS Groupware 4.2 are vulnerable.

Vulnerability Detection Method

Details: Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.100537)

Version used: $Revision: 5144 $

Product Detection Result

Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

References

CVE: CVE-2010-1135, CVE-2010-1134, CVE-2010-1133, CVE-2010-1136
BID: 38608
Other: http://www.securityfocus.com/bid/38608
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=24734
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25046
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25424
http://tikiwiki.svn.sourceforge.net/viewvc/tikiwiki?view=rev&revision=25435
http://info.tikiwiki.org/article86-Tiki-Announces-3-5-and-4-2-Releases
http://info.tikiwiki.org/tiki-index.php?page=homepage

High (CVSS: 7.5) 80/tcp
NVT: PHP-CGI-based setups vulnerability when parsing query string parameters from ph... (OID: 1.3.6.1.4.1.25623.1.0.103482)

Summary

PHP is prone to an information-disclosure vulnerability.

Vulnerability Detection Result

Vulnerable url: http://192.168.1.109/cgi-bin/php

Impact

Exploiting this issue allows remote attackers to view the source code of files in the context of the server process. This may allow the attacker to obtain sensitive information and to run arbitrary PHP code on the affected computer. Other attacks are also possible.

Solution

Solution type: VendorFix

PHP has released version 5.4.3 and 5.3.13 to address this vulnerability. PHP is recommending that users upgrade to the latest version of PHP.

Vulnerability Insight

When PHP is used in a CGI-based setup (such as Apache's mod_cgid), the php-cgi receives a processed query string parameter as command line arguments which allows command-line switches, such as -s, -d or -c to be passed to the php-cgi binary, which can be exploited to disclose source code and obtain arbitrary code execution.

An example of the -s command, allowing an attacker to view the source code of index.php is below:

http://localhost/index.php?-s

Vulnerability Detection Method

Details: PHP-CGI-based setups vulnerability when parsing query string parameters from ph... (OID: 1.3.6.1.4.1.25623.1.0.103482)

Version used: $Revision: 11457 $

References

CVE:	CVE-2012-1823, CVE-2012-2311, CVE-2012-2336, CVE-2012-2335
BID:	53388
CERT:	DFN-CERT-2013-1494, DFN-CERT-2012-1316, DFN-CERT-2012-1276, DFN-CERT-2012-1268, DFN-CERT-2012-1267, DFN-CERT-2012-1266, DFN-CERT-2012-1173, DFN-CERT-2012-1101, DFN-CERT-2012-0994, DFN-CERT-2012-0993, DFN-CERT-2012-0992, DFN-CERT-2012-0920, DFN-CERT-2012-0915, DFN-CERT-2012-0914, DFN-CERT-2012-0913, DFN-CERT-2012-0907, DFN-CERT-2012-0906, DFN-CERT-2012-0900, DFN-CERT-2012-0880, DFN-CERT-2012-0878
Other:	http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-1567532.html
	http://www.kb.cert.org/vuls/id/520827
	http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
	https://bugs.php.net/bug.php?id=61910
	http://www.php.net/manual/en/security.cgi-bin.php
	http://www.securityfocus.com/bid/53388

High (CVSS: 7.5) 6200/tcp
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103185)

Summary

vsftpd is prone to a backdoor vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution

Solution type: VendorFix

The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS

The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method

Details: vsftpd Compromised Source Packages Backdoor Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103185)

Version used: $Revision: 12076 $

References

BID:	48539
Other:	http://www.securityfocus.com/bid/48539
	http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
	https://security.appspot.com/vsftpd.html

High (CVSS: 7.5) 21/tcp
NVT: vsftpd Compromised Source Packages Backdoor Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103185)

Summary

vsftpd is prone to a backdoor vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected application.

Solution

Solution type: VendorFix

The repaired package can be downloaded from the referenced link. Please validate the package with its signature.

Affected Software/OS

The vsftpd 2.3.4 source package is affected.

Vulnerability Detection Method

Details: vsftpd Compromised Source Packages Backdoor Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.103185)

Version used: $Revision: 12076 $

References

BID:	48539
Other:	http://www.securityfocus.com/bid/48539
	http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
	https://security.appspot.com/vsftpd.html

High (CVSS: 7.5) 6667/tcp
NVT: Check for Backdoor in UnrealIRCd (OID: 1.3.6.1.4.1.25623.1.0.80111)

Summary

Detection of backdoor in UnrealIRCd.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Solution

Solution type: VendorFix

Install latest version of unrealircd and check signatures of software you're installing.

Vulnerability Insight

Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.

The issue affects Unreal 3.2.8.1 for Linux. Reportedly package Unreal3.2.8.1.tar.gz downloaded in November 2009 and later is affected. The MD5 sum of the affected file is 752e46f2d873c1679fa99de3f52a274d. Files with MD5 sum of 7b741e94e867c0a7370553fd01506c66 are not affected.

Vulnerability Detection Method

Details: Check for Backdoor in UnrealIRCd (OID: 1.3.6.1.4.1.25623.1.0.80111)

Version used: $Revision: 5433 $

References

CVE:	CVE-2010-2075
BID:	40820
Other:	http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt
	http://seclists.org/fulldisclosure/2010/Jun/277
	http://www.securityfocus.com/bid/40820

High (CVSS: 7.5) 80/tcp
NVT: Test HTTP dangerous methods (OID: 1.3.6.1.4.1.25623.1.0.10498)

Summary

Misconfigured web servers allows remote clients to perform dangerous HTTP methods such as PUT and DELETE. This script checks if they are enabled and can be misused to upload or delete files.

Vulnerability Detection Result

We could upload the following files via the PUT method at this web server:

http://192.168.1.109/dav/puttest2133722346.html

We could delete the following files via the DELETE method at this web server:

http://192.168.1.109/dav/puttest2133722346.html

Impact

- Enabled PUT method: This might allow an attacker to upload and run arbitrary code on this web server.

- Enabled DELETE method: This might allow an attacker to delete additional files on this web server.

Solution

Solution type: Mitigation

Use access restrictions to these dangerous HTTP methods or disable them completely.

Vulnerability Detection Method

Details: Test HTTP dangerous methods (OID: 1.3.6.1.4.1.25623.1.0.10498)

Version used: $Revision: 9335 $

References

BID: 12141
Other: OWASP:OWASP-CM-001

High (CVSS: 7.5) 22/tcp
NVT: SSH Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103239)

Summary

It was possible to login into the remote SSH server using default credentials.

As the NVT 'SSH Brute Force Logins with default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this NVT instead. The script preference 'Report timeout' allows you to configure if such an timeout is reported.

Vulnerability Detection Result

It was possible to login with the following credentials <User>:<Password>

msfadmin:msfadmin
user:user

Solution

Solution type: Mitigation

Change the password as soon as possible.

Vulnerability Detection Method

Try to login with a number of known default credentials via the SSH protocol.

Details: SSH Brute Force Logins With Default Credentials Reporting (OID: 1.3.6.1.4.1.25623.1.0.103239)

Version used: $Revision: 13568 $

Medium (CVSS: 6.8) 6667/tcp
NVT: UnrealIRCd Authentication Spoofing Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.809883)

Product detection result: cpe:/a:unrealircd:unrealircd:3.2.8.1 by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)

Summary

This host is installed with UnrealIRCd and is prone to authentication spoofing vulnerability.

Vulnerability Detection Result

Installed version: 3.2.8.1
Fixed version: 3.2.10.7

Impact

Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.

Solution

Solution type: VendorFix

Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.

Affected Software/OS

UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.

Vulnerability Insight

The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: UnrealIRCd Authentication Spoofing Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.809883)

Version used: $Revision: 11874 $

Product Detection Result

Product: cpe:/a:unrealircd:unrealircd:3.2.8.1
Method: UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)

References

CVE:	CVE-2016-7144
BID:	92763
Other:	http://seclists.org/oss-sec/2016/q3/420
	http://www.openwall.com/lists/oss-security/2016/09/05/8
	https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86bc50ba1a34a766
	https://bugs.unrealircd.org/main_page.php

Medium (CVSS: 6.8) 80/tcp
NVT: TWiki Cross-Site Request Forgery Vulnerability - Sep10 (OID: 1.3.6.1.4.1.25623.1.0.801281)

Product detection result: cpe:/a:twiki:twiki:01.Feb.2003 by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary

The host is running TWiki and is prone to Cross-Site Request Forgery vulnerability.

Vulnerability Detection Result

Installed version: 01.Feb.2003
Fixed version: 4.3.2

Impact

Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution

Solution type: VendorFix

Upgrade to TWiki version 4.3.2 or later.

Affected Software/OS

TWiki version prior to 4.3.2

Vulnerability Insight

Attack can be done by tricking an authenticated TWiki user into visiting a static HTML page on another side, where a Javascript enabled browser will send an HTTP POST request to TWiki, which in turn will process the request as the TWiki user.

Vulnerability Detection Method

Details: TWiki Cross-Site Request Forgery Vulnerability - Sep10 (OID: 1.3.6.1.4.1.25623.1.0.801281)

Version used: $Revision: 12952 $

Product Detection Result

Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

References

CVE: CVE-2009-4898
Other: http://www.openwall.com/lists/oss-security/2010/08/03/8
http://www.openwall.com/lists/oss-security/2010/08/02/17
http://twiki.org/cgi-bin/view/Codev/SecurityAuditTokenBasedCsrfFix
http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Medium (CVSS: 6.8) 5432/tcp
NVT: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)

Summary

OpenSSL is prone to security-bypass vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successfully exploiting this issue may allow attackers to obtain sensitive information by conducting a man-in-the-middle attack. This may lead to other attacks.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m and 1.0.1 before 1.0.1h.

Vulnerability Insight

OpenSSL does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the 'CCS Injection' vulnerability.

Vulnerability Detection Method

Send two SSL ChangeCipherSpec request and check the response.

Details: SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.105042)

Version used: $Revision: 12865 $

References

CVE:	CVE-2014-0224
BID:	67899
CERT:	CB-K15/0567, CB-K15/0415, CB-K15/0384, CB-K15/0080, CB-K15/0079, CB-K15/0074, CB-K14/1617, CB-K14/1537, CB-K14/1299, CB-K14/1297, CB-K14/1294, CB-K14/1202, CB-K14/1174, CB-K14/1153, CB-K14/0876, CB-K14/0756, CB-K14/0746, CB-K14/0736, CB-K14/0722, CB-K14/0716, CB-K14/0708, CB-K14/0684, CB-K14/0683, CB-K14/0680, DFN-CERT-2016-0388, DFN-CERT-2015-0593, DFN-CERT-2015-0427, DFN-CERT-2015-0396, DFN-CERT-2015-0082, DFN-CERT-2015-0079, DFN-CERT-2015-0078, DFN-CERT-2014-1717, DFN-CERT-2014-1632, DFN-CERT-2014-1364, DFN-CERT-2014-1357, DFN-CERT-2014-1350, DFN-CERT-2014-1265, DFN-CERT-2014-1209, DFN-CERT-2014-0917, DFN-CERT-2014-0789, DFN-CERT-2014-0778, DFN-CERT-2014-0768, DFN-CERT-2014-0752, DFN-CERT-2014-0747, DFN-CERT-2014-0738, DFN-CERT-2014-0715, DFN-CERT-2014-0714, DFN-CERT-2014-0709
Other:	https://www.openssl.org/news/secadv/20140605.txt http://www.securityfocus.com/bid/67899 http://openssl.org/

Medium (CVSS: 6.8) 25/tcp
NVT: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection ... (OID: 1.3.6.1.4.1.25623.1.0.103935)

Summary

Multiple vendors' implementations of 'STARTTLS' are prone to a vulnerability that lets attackers inject arbitrary commands.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker can exploit this issue to execute arbitrary commands in the context of the user running the application. Successful exploits can allow attackers to obtain email usernames and passwords.

Solution

Solution type: VendorFix

Updates are available. Please see the references for more information.

Affected Software/OS

The following vendors are affected:

Ipswitch

Kerio

Postfix

Qmail-TLS

Oracle

SCO Group

spamdyke

ISC

Vulnerability Detection Method

Send a special crafted 'STARTTLS' request and check the response.

Details: Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection ... (OID: 1.3.6.1.4.1.25623.1.0.103935)

Version used: $Revision: 13204 $

References

CVE:	CVE-2011-0411, CVE-2011-1430, CVE-2011-1431, CVE-2011-1432, CVE-2011-1506, CVE-2011-1575, CVE-2011-1926, CVE-2011-2165
BID:	46767
CERT:	CB-K15/1514, DFN-CERT-2011-0917, DFN-CERT-2011-0912, DFN-CERT-2011-0897, DFN-CERT-2011-0844, DFN-CERT-2011-0818, DFN-CERT-2011-0808, DFN-CERT-2011-0771, DFN-CERT-2011-0741, DFN-CERT-2011-0712, DFN-CERT-2011-0673, DFN-CERT-2011-0597, DFN-CERT-2011-0596, DFN-CERT-2011-0519, DFN-CERT-2011-0516, DFN-CERT-2011-0483, DFN-CERT-2011-0434, DFN-CERT-2011-0393, DFN-CERT-2011-0381
Other:	http://www.securityfocus.com/bid/46767
	http://kolab.org/pipermail/kolab-announce/2011/000101.html
	http://bugzilla.cyrusimap.org/show_bug.cgi?id=3424
	http://cyrusimap.org/mediawiki/index.php/Bugs_Resolved_in_2.4.7
	http://www.kb.cert.org/vuls/id/MAPG-8D9M4P

http://files.kolab.org/server/release/kolab-server-2.3.2/sources/release-notes.txt
http://www.postfix.org/CVE-2011-0411.html
http://www.pureftpd.org/project/pure-ftpd/news
http://www.watchguard.com/support/release-notes/xcs/9/en-US/EN_ReleaseNotes_XCS_9_1_1/EN_ReleaseNotes_WG_XCS_9_1_TLS_Hotfix.pdf
http://www.spamdyke.org/documentation/Changelog.txt
http://datatracker.ietf.org/doc/draft-josefsson-kerberos5-starttls/?include_text=1
http://www.securityfocus.com/archive/1/516901
http://support.avaya.com/css/P8/documents/100134676
http://support.avaya.com/css/P8/documents/100141041
http://www.oracle.com/technetwork/topics/security/cpuapr2011-301950.html
http://inoa.net/qmail-tls/vu555316.patch
http://www.kb.cert.org/vuls/id/555316

Medium (CVSS: 6.5) 80/tcp
NVT: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141885)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary

In Tiki the user task component is vulnerable to a SQL Injection via the tiki-user_tasks.php show_history parameter.

Vulnerability Detection Result

Installed version: 1.9.5
Fixed version: 17.2

Solution

Solution type: VendorFix

Upgrade to version 17.2 or later.

Affected Software/OS

Tiki Wiki CMS Groupware prior to version 17.2.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Tiki Wiki CMS Groupware < 17.2 SQL Injection Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141885)

Version used: $Revision: 13115 $

Product Detection Result

Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

References

CVE: CVE-2018-20719
Other: https://blog.ripstech.com/2018/scan-verify-patch-security-issues-in-minutes/

Medium (CVSS: 6.4) 21/tcp
NVT: Anonymous FTP Login Reporting (OID: 1.3.6.1.4.1.25623.1.0.900600)

Summary

Reports if the remote FTP Server allows anonymous logins.

Vulnerability Detection Result

It was possible to login to the remote FTP service with the following anonymous account(s):

anonymous:anonymous@example.com
ftp:anonymous@example.com

Impact

Based on the files accessible via this anonymous FTP login and the permissions of this account an attacker might be able to:

- gain access to sensitive files

- upload or delete files.

Solution

Solution type: Mitigation

If you do not want to share files, you should disable anonymous logins.

Vulnerability Insight

A host that provides an FTP service may additionally provide Anonymous FTP access as well. Under this arrangement, users do not strictly need an account on the host. Instead the user typically enters 'anonymous' or 'ftp' when prompted for username. Although users are commonly asked to send their email address as their password, little to no verification is actually performed on the supplied data.

Vulnerability Detection Method

Details: Anonymous FTP Login Reporting (OID: 1.3.6.1.4.1.25623.1.0.900600)

Version used: $Revision: 12030 $

References

Other: https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

Medium (CVSS: 6.0) 80/tcp
NVT: TWiki Cross-Site Request Forgery Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800400)

Product detection result: cpe:/a:twiki:twiki:01.Feb.2003 by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary

The host is running TWiki and is prone to Cross-Site Request Forgery Vulnerability.

Vulnerability Detection Result

Installed version: 01.Feb.2003
Fixed version: 4.3.1

Impact

Successful exploitation will allow attacker to gain administrative privileges on the target application and can cause CSRF attack.

Solution

Solution type: VendorFix

Upgrade to version 4.3.1 or later.

Affected Software/OS

TWiki version prior to 4.3.1

Vulnerability Insight

Remote authenticated user can create a specially crafted image tag that, when viewed by the target user, will update pages on the target system with the privileges of the target user via HTTP requests.

Vulnerability Detection Method

Details: TWiki Cross-Site Request Forgery Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800400)

Version used: $Revision: 12952 $

Product Detection Result

Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

References

CVE: CVE-2009-1339
Other: http://secunia.com/advisories/34880
http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=526258
http://twiki.org/p/pub/Codev/SecurityAlert-CVE-2009-1339/TWiki-4.3.0-c-diff-cve-2009-1339.txt

Medium (CVSS: 6.0) 445/tcp
NVT: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check) (OID: 1.3.6.1.4.1.25623.1.0.108011)

Product detection result: cpe:/a:samba:samba:3.0.20 by SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

Summary

Samba is prone to a vulnerability that allows attackers to execute arbitrary shell commands because the software fails to sanitize user-supplied input.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker may leverage this issue to execute arbitrary shell commands on an affected system with the privileges of the application.

Solution

Solution type: VendorFix

Updates are available. Please see the referenced vendor advisory.

Affected Software/OS

This issue affects Samba 3.0.0 to 3.0.25rc3.

Vulnerability Detection Method

Send a crafted command to the samba server and check for a remote command execution.

Details: Samba MS-RPC Remote Shell Command Execution Vulnerability (Active Check) (OID: 1.3.6.1.4.1.25623.1.0.108011)

Version used: $Revision: 10398 $

Product Detection Result

Product: cpe:/a:samba:samba:3.0.20
Method: SMB NativeLanMan (OID: 1.3.6.1.4.1.25623.1.0.102011)

References

CVE:	CVE-2007-2447
BID:	23972
Other:	http://www.securityfocus.com/bid/23972
	https://www.samba.org/samba/security/CVE-2007-2447.html

Medium (CVSS: 5.8) 80/tcp
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled (OID: 1.3.6.1.4.1.25623.1.0.11213)

Summary

Debugging functions are enabled on the remote web server.

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

Vulnerability Detection Result

The web server has the following HTTP methods enabled: TRACE

Impact

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution type: Mitigation

Disable the TRACE and TRACK methods in your web server configuration.

Please see the manual of your web server or the references for more information.

Affected Software/OS

Web servers with enabled TRACE and/or TRACK methods.

Vulnerability Insight

It has been shown that web servers supporting this methods are subject to cross-site-scripting attacks, dubbed XST for Cross-Site-Tracing, when used in conjunction with various weaknesses in browsers.

Vulnerability Detection Method

Details: HTTP Debugging Methods (TRACE/TRACK) Enabled (OID: 1.3.6.1.4.1.25623.1.0.11213)

Version used: $Revision: 10828 $

References

CVE:	CVE-2003-1567, CVE-2004-2320, CVE-2004-2763, CVE-2005-3398, CVE-2006-4683, CVE-2007-3008, CVE-2008-7253, CVE-2009-2823, CVE-2010-0386, CVE-2012-2223, CVE-2014-7883
BID:	9506, 9561, 11604, 15222, 19915, 24456, 33374, 36956, 36990, 37995
CERT:	CB-K14/0981, DFN-CERT-2014-1018, DFN-CERT-2010-0020
Other:	http://www.kb.cert.org/vuls/id/288308
	http://www.kb.cert.org/vuls/id/867593
	http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
	https://www.owasp.org/index.php/Cross_Site_Tracing

Medium (CVSS: 5.0) 25/tcp
NVT: Check if Mailserver answer to VRFY and EXPN requests (OID: 1.3.6.1.4.1.25623.1.0.100072)

Summary

The Mailserver on this host answers to VRFY and/or EXPN requests.

Vulnerability Detection Result

'VRFY root' produces the following answer: 252 2.0.0 root

Solution

Solution type: Workaround

Disable VRFY and/or EXPN on your Mailserver.

For postfix add 'disable_vrfy_command=yes' in 'main.cf'.

For Sendmail add the option 'O PrivacyOptions=goaway'.

It is suggested that, if you really want to publish this type of information, you use a mechanism that legitimate users actually know about, such as Finger or HTTP.

Vulnerability Insight

VRFY and EXPN ask the server for information about an address. They are inherently unusable through firewalls, gateways, mail exchangers for part-time hosts, etc.

Vulnerability Detection Method

Details: Check if Mailserver answer to VRFY and EXPN requests (OID: 1.3.6.1.4.1.25623.1.0.100072)

Version used: $Revision: 13470 $

References

Other: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 5.0) 25/tcp
NVT: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

The certificate of the remote service expired on 2010-04-16 14:07:45.

Certificate details:
subject ...:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
subject alternative names (SAN):
None
issued by .:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

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

Vulnerability Detection Method

Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Version used: $Revision: 11103 $

Medium (CVSS: 5.0) 5432/tcp
NVT: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Summary

The remote server's SSL/TLS certificate has already expired.

Vulnerability Detection Result

The certificate of the remote service expired on 2010-04-16 14:07:45.

Certificate details:
subject ...:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
subject alternative names (SAN):
None
issued by .:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
serial ....: 00FAF93A4C7FB6B9CC
valid from : 2010-03-17 14:07:45 UTC
valid until: 2010-04-16 14:07:45 UTC
fingerprint (SHA-1): ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256): E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7AF1E32DEE436DE813CC

Solution

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

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

Vulnerability Detection Method

Details: SSL/TLS: Certificate Expired (OID: 1.3.6.1.4.1.25623.1.0.103955)

Version used: $Revision: 11103 $

Medium (CVSS: 5.0) 80/tcp
NVT: TWiki < 6.1.0 XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141830)

Product detection result: cpe:/a:twiki:twiki:01.Feb.2003 by TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

Summary

bin/statistics in TWiki 6.0.2 allows XSS via the webs parameter.

Vulnerability Detection Result

Installed version: 01.Feb.2003
Fixed version: 6.1.0

Solution

Solution type: VendorFix

Update to version 6.1.0 or later.

Affected Software/OS

TWiki version 6.0.2 and probably prior.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: TWiki < 6.1.0 XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.141830)

Version used: $Revision: 12952 $

Product Detection Result

Product: cpe:/a:twiki:twiki:01.Feb.2003
Method: TWiki Version Detection (OID: 1.3.6.1.4.1.25623.1.0.800399)

References

CVE:	CVE-2018-20212
Other:	https://seclists.org/fulldisclosure/2019/Jan/7
	http://twiki.org/cgi-bin/view/Codev/DownloadTWiki

Medium (CVSS: 5.0) 80/tcp
NVT: /doc directory browsable (OID: 1.3.6.1.4.1.25623.1.0.10056)

Summary

The /doc directory is browsable. /doc shows the content of the /usr/doc directory and therefore it shows which programs and - important! - the version of the installed programs.

Vulnerability Detection Result

Vulnerable url: http://192.168.1.109/doc/

Solution

Solution type: Mitigation

Use access restrictions for the /doc directory. If you use Apache you might use this in your access.conf:

<Directory /usr/doc> AllowOverride None order deny,allow deny from all allow from localhost </Directory>

Vulnerability Detection Method

Details: /doc directory browsable (OID: 1.3.6.1.4.1.25623.1.0.10056)

Version used: $Revision: 4288 $

References

CVE:	CVE-1999-0678
BID:	318

Medium (CVSS: 5.0) 80/tcp
NVT: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800315)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary

The host is installed with Tiki Wiki CMS Groupware and is prone to input sanitation weakness vulnerability.

Vulnerability Detection Result

Installed version: 1.9.5
Fixed version: 2.2

Impact

Successful exploitation could allow arbitrary code execution in the context of an affected site.

Impact Level: Application

Solution

Solution type: VendorFix

Upgrade to version 2.2 or latest http://info.tikiwiki.org/tiki-index.php?page=Get+Tiki&bl

Affected Software/OS

Tiki Wiki CMS Groupware version prior to 2.2 on all running platform

Vulnerability Insight

The vulnerability is due to input validation error in tiki-error.php which fails to sanitise before being returned to the user.

Vulnerability Detection Method

Details: Tiki Wiki CMS Groupware Input Sanitation Weakness Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.800315)

Version used: $Revision: 5144 $

Product Detection Result

Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

References

CVE: CVE-2008-5318, CVE-2008-5319
Other: http://secunia.com/advisories/32341
http://info.tikiwiki.org/tiki-read_article.php?articleId=41

Medium (CVSS: 5.0) 80/tcp
NVT: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.108064)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary

The host is installed with Tiki Wiki CMS Groupware and is prone to a local file inclusion vulnerability.

Vulnerability Detection Result

Installed version: 1.9.5
Fixed version: 12.11

Impact

Successful exploitation will allow an user having access to the admin backend to gain access to arbitrary files and to compromise the application.

Solution

Solution type: VendorFix

Upgrade to Tiki Wiki CMS Groupware version 12.11 LTS, 15.4 or later.

Affected Software/OS

Tiki Wiki CMS Groupware versions:

- below 12.11 LTS

- 13.x, 14.x and 15.x below 15.4

Vulnerability Insight

The Flaw is due to improper sanitization of input passed to the 'fixedURLData' parameter of the 'display_banner.php' script.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Tiki Wiki CMS Groupware 'fixedURLData' Local File Inclusion Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.108064)

Version used: $Revision: 11863 $

Product Detection Result

Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

References

CVE: CVE-2016-10143
Other: http://tiki.org/article445-Security-updates-Tiki-16-2-15-4-and-Tiki-12-11-released
https://sourceforge.net/p/tikiwiki/code/60308/
https://tiki.org

Medium (CVSS: 5.0) 80/tcp
NVT: awiki Multiple Local File Include Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.103210)

Summary

awiki is prone to multiple local file-include vulnerabilities because it fails to properly sanitize user-supplied input.

Vulnerability Detection Result

Vulnerable url: http://192.168.1.109/mutillidae/index.php?page=/etc/passwd

Impact

An attacker can exploit this vulnerability to obtain potentially sensitive information and execute arbitrary local scripts in the context of the webserver process. This may allow the attacker to compromise the application and the host. Other attacks are also possible.

Solution

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

awiki 20100125 is vulnerable. Other versions may also be affected.

Vulnerability Detection Method

Details: awiki Multiple Local File Include Vulnerabilities (OID: 1.3.6.1.4.1.25623.1.0.103210)

Version used: $Revision: 10741 $

References

BID:	49187
Other:	https://www.exploit-db.com/exploits/36047/
	http://www.securityfocus.com/bid/49187
	http://www.kobaonline.com/awiki/

Medium (CVSS: 4.8) 5900/tcp
NVT: VNC Server Unencrypted Data Transmission (OID: 1.3.6.1.4.1.25623.1.0.108529)

Summary

The remote host is running a VNC server providing one or more insecure or cryptographically weak Security Type(s) not intended for use on untrusted networks.

Vulnerability Detection Result

The VNC server provides the following insecure or cryptographically weak Security Type(s):

2 (VNC authentication)

Impact

An attacker can uncover sensitive data by sniffing traffic to the VNC server.

Solution

Solution type: Mitigation

Run the session over an encrypted channel provided by IPsec [RFC4301] or SSH [RFC4254]. Some VNC server vendors are also providing more secure Security Types within their products.

Vulnerability Detection Method

Details: VNC Server Unencrypted Data Transmission (OID: 1.3.6.1.4.1.25623.1.0.108529)

Version used: $Revision: 13014 $

References

Other: https://tools.ietf.org/html/rfc6143#page-10

Medium (CVSS: 4.8) 23/tcp
NVT: Telnet Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108522)

Summary

The remote host is running a Telnet service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

An attacker can uncover login names and passwords by sniffing traffic to the Telnet service.

Solution

Solution type: Mitigation

Replace Telnet with a protocol like SSH which supports encrypted connections.

Vulnerability Detection Method

Details: Telnet Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108522)

Version used: $Revision: 13366 $

Medium (CVSS: 4.8) 2121/tcp
NVT: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)

Summary

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Anonymous sessions: 331 Password required for anonymous
Non-anonymous sessions: 331 Password required for openvas-vt

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)

Version used: $Revision: 13026 $

Medium (CVSS: 4.8) 21/tcp
NVT: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)

Summary

The remote host is running a FTP service that allows cleartext logins over unencrypted connections.

Vulnerability Detection Result

The remote FTP service accepts logins without a previous sent 'AUTH TLS' command. Response(s):

Anonymous sessions: 331 Please specify the password.
Non-anonymous sessions: 331 Please specify the password.

Impact

An attacker can uncover login names and passwords by sniffing traffic to the FTP service.

Solution

Solution type: Mitigation

Enable FTPS or enforce the connection via the 'AUTH TLS' command. Please see the manual of the FTP service for more information.

Vulnerability Detection Method

Tries to login to a non FTPS enabled FTP service without sending a 'AUTH TLS' command first and checks if the service is accepting the login without enforcing the use of the 'AUTH TLS' command.

Details: FTP Unencrypted Cleartext Login (OID: 1.3.6.1.4.1.25623.1.0.108528)

Version used: $Revision: 13026 $

Medium (CVSS: 4.8) 80/tcp
NVT: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440)

Summary

The host / application transmits sensitive information (username, passwords) in cleartext via HTTP.

Vulnerability Detection Result

The following input fields where identified (URL:input name):

http://192.168.1.109/phpMyAdmin/:pma_password
http://192.168.1.109/phpMyAdmin/?D=A:pma_password
http://192.168.1.109/tikiwiki/tiki-install.php:pass
http://192.168.1.109/twiki/bin/view/TWiki/TWikiUserAuthentication:oldpassword

Impact

An attacker could use this situation to compromise or eavesdrop on the HTTP communication between the client and the server using a man-in-the-middle attack to get access to sensitive data like usernames or passwords.

Solution

Solution type: Workaround

Enforce the transmission of sensitive data via an encrypted SSL/TLS connection. Additionally make sure the host / application is redirecting all users to the secured SSL/TLS connection before allowing to input sensitive data into the mentioned functions.

Affected Software/OS

Hosts / applications which doesn't enforce the transmission of sensitive data via an encrypted SSL/TLS connection.

Vulnerability Detection Method

Evaluate previous collected information and check if the host / application is not enforcing the transmission of sensitive data via an encrypted SSL/TLS connection.

The script is currently checking the following:

- HTTP Basic Authentication (Basic Auth)

- HTTP Forms (e.g. Login) with input field of type 'password'

Details: Cleartext Transmission of Sensitive Information via HTTP (OID: 1.3.6.1.4.1.25623.1.0.108440)

Version used: $Revision: 10726 $

References

Other: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Session_Management
https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
https://cwe.mitre.org/data/definitions/319.html

Medium (CVSS: 4.3) 5432/tcp
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ... (OID: 1.3.6.1.4.1.25623.1.0.802087)

Summary

This host is prone to an information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution

Solution type: Mitigation

Possible Mitigations are:

- Disable SSLv3

- Disable cipher suites supporting CBC cipher modes

- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Evaluate previous collected information about this service.

Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ... (OID: 1.3.6.1.4.1.25623.1.0.802087)

Version used: $Revision: 11402 $

References

CVE:	CVE-2014-3566
BID:	70574
CERT:	CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1102, CB-K16/0599, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0642, DFN-CERT-2016-0388, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354
Other:	https://www.openssl.org/~bodo/ssl-poodle.pdf https://www.imperialviolet.org/2014/10/14/poodle.html https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

Medium (CVSS: 4.3) 25/tcp
NVT: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ... (OID: 1.3.6.1.4.1.25623.1.0.802087)

Summary

This host is prone to an information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow a man-in-the-middle attackers gain access to the plain text data stream.

Solution

Solution type: Mitigation

Possible Mitigations are:

- Disable SSLv3

- Disable cipher suites supporting CBC cipher modes

- Enable TLS_FALLBACK_SCSV if the service is providing TLSv1.0+

Vulnerability Insight

The flaw is due to the block cipher padding not being deterministic and not covered by the Message Authentication Code

Vulnerability Detection Method

Evaluate previous collected information about this service.

Details: SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability ... (OID: 1.3.6.1.4.1.25623.1.0.802087)

Version used: $Revision: 11402 $

References

CVE:	CVE-2014-3566
BID:	70574
CERT:	CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1102, CB-K16/0599, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0642, DFN-CERT-2016-0388, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354
Other:	https://www.openssl.org/~bodo/ssl-poodle.pdf https://www.imperialviolet.org/2014/10/14/poodle.html https://www.dfranke.us/posts/2014-10-14-how-poodle-happened.html http://googleonlinesecurity.blogspot.in/2014/10/this-poodle-bites-exploiting-ssl-30.html

Medium (CVSS: 4.3) 5432/tcp
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1.0+ the service is also providing the deprecated SSLv3 protocol and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution

Solution type: Mitigation

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:

- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)

- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method

Check the used protocols of the services provided by this system.

Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Version used: $Revision: 5547 $

References

CVE: CVE-2016-0800, CVE-2014-3566

CERT: CB-K18/0094, CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1141, CB-K16/1107, CB-K16/1102, CB-K16/0792, CB-K16/0599, CB-K16/0597, CB-K16/0459, CB-K16/0456, CB-K16/0433, CB-K16/0424, CB-K16/0415, CB-K16/0413, CB-K16/0374, CB-K16/0367, CB-K16/0331, CB-K16/0329, CB-K16/0328, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2018-0096, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1216, DFN-CERT-2016-1174, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0841, DFN-CERT-2016-0644, DFN-CERT-2016-0642, DFN-CERT-2016-0496, DFN-CERT-2016-0495, DFN-CERT-2016-0465, DFN-CERT-2016-0459, DFN-CERT-2016-0453, DFN-CERT-2016-0451, DFN-CERT-2016-0415, DFN-CERT-2016-0403, DFN-CERT-2016-0388, DFN-CERT-2016-0360, DFN-CERT-2016-0359, DFN-CERT-2016-0357, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354

Other: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://drownattack.com/
https://www.imperialviolet.org/2014/10/14/poodle.html

Medium (CVSS: 4.3) 25/tcp
NVT: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Summary

It was possible to detect the usage of the deprecated SSLv2 and/or SSLv3 protocol on this system.

Vulnerability Detection Result

In addition to TLSv1.0+ the service is also providing the deprecated SSLv2 and SSLv3 protocols and supports one or more ciphers. Those supported ciphers can be found in the 'SSL/TLS: Report Weak and Supported Ciphers' (OID: 1.3.6.1.4.1.25623.1.0.802067) NVT.

Impact

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Solution

Solution type: Mitigation

It is recommended to disable the deprecated SSLv2 and/or SSLv3 protocols in favor of the TLSv1+ protocols. Please see the references for more information.

Affected Software/OS

All services providing an encrypted communication using the SSLv2 and/or SSLv3 protocols.

Vulnerability Insight

The SSLv2 and SSLv3 protocols containing known cryptographic flaws like:

- Padding Oracle On Downgraded Legacy Encryption (POODLE, CVE-2014-3566)

- Decrypting RSA with Obsolete and Weakened eNcryption (DROWN, CVE-2016-0800)

Vulnerability Detection Method

Check the used protocols of the services provided by this system.

Details: SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection (OID: 1.3.6.1.4.1.25623.1.0.111012)

Version used: $Revision: 5547 $

References

CVE: CVE-2016-0800, CVE-2014-3566

CERT: CB-K18/0094, CB-K17/1198, CB-K17/1196, CB-K16/1828, CB-K16/1438, CB-K16/1384, CB-K16/1141, CB-K16/1107, CB-K16/1102, CB-K16/0792, CB-K16/0599, CB-K16/0597, CB-K16/0459, CB-K16/0456, CB-K16/0433, CB-K16/0424, CB-K16/0415, CB-K16/0413, CB-K16/0374, CB-K16/0367, CB-K16/0331, CB-K16/0329, CB-K16/0328, CB-K16/0156, CB-K15/1514, CB-K15/1358, CB-K15/1021, CB-K15/0972, CB-K15/0637, CB-K15/0590, CB-K15/0525, CB-K15/0393, CB-K15/0384, CB-K15/0287, CB-K15/0252, CB-K15/0246, CB-K15/0237, CB-K15/0118, CB-K15/0110, CB-K15/0108, CB-K15/0080, CB-K15/0078, CB-K15/0077, CB-K15/0075, CB-K14/1617, CB-K14/1581, CB-K14/1537, CB-K14/1479, CB-K14/1458, CB-K14/1342, CB-K14/1314, CB-K14/1313, CB-K14/1311, CB-K14/1304, CB-K14/1296, DFN-CERT-2018-0096, DFN-CERT-2017-1238, DFN-CERT-2017-1236, DFN-CERT-2016-1929, DFN-CERT-2016-1527, DFN-CERT-2016-1468, DFN-CERT-2016-1216, DFN-CERT-2016-1174, DFN-CERT-2016-1168, DFN-CERT-2016-0884, DFN-CERT-2016-0841, DFN-CERT-2016-0644, DFN-CERT-2016-0642, DFN-CERT-2016-0496, DFN-CERT-2016-0495, DFN-CERT-2016-0465, DFN-CERT-2016-0459, DFN-CERT-2016-0453, DFN-CERT-2016-0451, DFN-CERT-2016-0415, DFN-CERT-2016-0403, DFN-CERT-2016-0388, DFN-CERT-2016-0360, DFN-CERT-2016-0359, DFN-CERT-2016-0357, DFN-CERT-2016-0171, DFN-CERT-2015-1431, DFN-CERT-2015-1075, DFN-CERT-2015-1026, DFN-CERT-2015-0664, DFN-CERT-2015-0548, DFN-CERT-2015-0404, DFN-CERT-2015-0396, DFN-CERT-2015-0259, DFN-CERT-2015-0254, DFN-CERT-2015-0245, DFN-CERT-2015-0118, DFN-CERT-2015-0114, DFN-CERT-2015-0083, DFN-CERT-2015-0082, DFN-CERT-2015-0081, DFN-CERT-2015-0076, DFN-CERT-2014-1717, DFN-CERT-2014-1680, DFN-CERT-2014-1632, DFN-CERT-2014-1564, DFN-CERT-2014-1542, DFN-CERT-2014-1414, DFN-CERT-2014-1366, DFN-CERT-2014-1354

Other: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report

https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://drownattack.com/
https://www.imperialviolet.org/2014/10/14/poodle.html

Medium (CVSS: 4.3) 25/tcp
NVT: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) (OID: 1.3.6.1.4.1.25623.1.0.805188)

Summary

This host is accepting 'DHE_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result

'DHE_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

'DHE_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

Impact

Successful exploitation will allow a man-in-the-middle attacker to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution

Solution type: VendorFix

- Remove support for 'DHE_EXPORT' cipher suites from the service

- If running OpenSSL updateto version 1.0.2b or 1.0.1n or later.

Affected Software/OS

- Hosts accepting 'DHE_EXPORT' cipher suites

- OpenSSL version before 1.0.2b and 1.0.1n

Vulnerability Insight

Flaw is triggered when handling Diffie-Hellman key exchanges defined in the 'DHE_EXPORT' cipher suites.

Vulnerability Detection Method

Check previous collected cipher suites saved in the KB.

Details: SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam) (OID: 1.3.6.1.4.1.25623.1.0.805188)

Version used: $Revision: 11872 $

References

CVE:	CVE-2015-4000
BID:	74733

CERT: CB-K16/1593, CB-K16/1552, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0964, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0877, CB-K15/0834, CB-K15/0802, CB-K15/0733, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1016, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0925, DFN-CERT-2015-0879, DFN-CERT-2015-0844, DFN-CERT-2015-0737

Other: https://weakdh.org

https://weakdh.org/imperfect-forward-secrecy.pdf

http://openwall.com/lists/oss-security/2015/05/20/8

https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained

https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes

Medium (CVSS: 4.3) 25/tcp
NVT: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142)

Summary

This host is accepting 'RSA_EXPORT' cipher suites and is prone to man in the middle attack.

Vulnerability Detection Result

'RSA_EXPORT' cipher suites accepted by this service via the SSLv3 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

'RSA_EXPORT' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5

Impact

Successful exploitation will allow remote attacker to downgrade the security of a session to use 'RSA_EXPORT' cipher suites, which are significantly weaker than non-export cipher suites. This may allow a man-in-the-middle attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

Solution

Solution type: VendorFix

- Remove support for 'RSA_EXPORT' cipher suites from the service.

- If running OpenSSL update to version 0.9.8zd or 1.0.0p or 1.0.1k or later.

Affected Software/OS

- Hosts accepting 'RSA_EXPORT' cipher suites

- OpenSSL version before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k.

Vulnerability Insight

Flaw is due to improper handling RSA temporary keys in a non-export RSA key exchange cipher suite.

Vulnerability Detection Method

Check previous collected cipher suites saved in the KB.

Details: SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK) (OID: 1.3.6.1.4.1.25623.1.0.805142)

Version used: $Revision: 11872 $

References

CVE:	CVE-2015-0204
BID:	71936
CERT:	CB-K18/0799, CB-K16/1289, CB-K16/1096, CB-K15/1751, CB-K15/1266, CB-K15/0850, CB-K15/0764, CB-K15/0720, CB-K15/0548, CB-K15/0526, CB-K15/0509, CB-K15/0493, CB-K15/0384, CB-K15/0365, CB-K15/0364, CB-K15/0302, CB-K15/0192, CB-K15/0016, DFN-CERT-2018-1408, DFN-CERT-2016-1372, DFN-CERT-2016-1164, DFN-CERT-2016-0388, DFN-CERT-2015-1853, DFN-CERT-2015-1332, DFN-CERT-2015-0884, DFN-CERT-2015-0800, DFN-CERT-2015-0758, DFN-CERT-2015-0567, DFN-CERT-2015-0544, DFN-CERT-2015-0530, DFN-CERT-2015-0396, DFN-CERT-2015-0375, DFN-CERT-2015-0374, DFN-CERT-2015-0305, DFN-CERT-2015-0199, DFN-CERT-2015-0021

Other: https://freakattack.com
http://secpod.org/blog/?p=3818
http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
https://www.openssl.org

Medium (CVSS: 4.3) 5432/tcp
NVT: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

Summary

This routine reports all Weak SSL/TLS cipher suites accepted by a service.

NOTE: No severity for SMTP services with 'Opportunistic TLS' and weak cipher suites on port 25/tcp is reported. If too strong cipher suites are configured for this service the alternative would be to fall back to an even more insecure cleartext communication.

Vulnerability Detection Result

'Weak' cipher suites accepted by this service via the SSLv3 protocol:

TLS_RSA_WITH_RC4_128_SHA

'Weak' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_RSA_WITH_RC4_128_SHA

Solution

Solution type: Mitigation

The configuration of this services should be changed so that it does not accept the listed weak cipher suites anymore.

Please see the references for more resources supporting you with this task.

Vulnerability Insight

These rules are applied for the evaluation of the cryptographic strength:

- RC4 is considered to be weak (CVE-2013-2566, CVE-2015-2808).

- Ciphers using 64 bit or less are considered to be vulnerable to brute force methods and therefore considered as weak (CVE-2015-4000).

- 1024 bit RSA authentication is considered to be insecure and therefore as weak.

- Any cipher considered to be secure for only the next 10 years is considered as medium

- Any other cipher is considered as strong

Vulnerability Detection Method

Details: SSL/TLS: Report Weak Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.103440)

Version used: $Revision: 11135 $

References

CVE: CVE-2013-2566, CVE-2015-2808, CVE-2015-4000

CERT: CB-K17/1750, CB-K16/1593, CB-K16/1552, CB-K16/1102, CB-K16/0617, CB-K16/0599, CB-K16/0168, CB-K16/0121, CB-K16/0090, CB-K16/0030, CB-K15/1751, CB-K15/1591, CB-K15/1550, CB-K15/1517, CB-K15/1514, CB-K15/1464, CB-K15/1442, CB-K15/1334, CB-K15/1269, CB-K15/1136, CB-K15/1090, CB-K15/1059, CB-K15/1022, CB-K15/1015, CB-K15/0986, CB-K15/0964, CB-K15/0962, CB-K15/0932, CB-K15/0927, CB-K15/0926, CB-K15/0907, CB-K15/0901, CB-K15/0896, CB-K15/0889, CB-K15/0877, CB-K15/0850, CB-K15/0849, CB-K15/0834, CB-K15/0827, CB-K15/0802, CB-K15/0764, CB-K15/0733, CB-K15/0667, CB-K14/0935, CB-K13/0942, DFN-CERT-2017-1821, DFN-CERT-2016-1692, DFN-CERT-2016-1648, DFN-CERT-2016-1168, DFN-CERT-2016-0665, DFN-CERT-2016-0642, DFN-CERT-2016-0184, DFN-CERT-2016-0135, DFN-CERT-2016-0101, DFN-CERT-2016-0035, DFN-CERT-2015-1853, DFN-CERT-2015-1679, DFN-CERT-2015-1632, DFN-CERT-2015-1608, DFN-CERT-2015-1542, DFN-CERT-2015-1518, DFN-CERT-2015-1406, DFN-CERT-2015-1341, DFN-CERT-2015-1194, DFN-CERT-2015-1144, DFN-CERT-2015-1113, DFN-CERT-2015-1078, DFN-CERT-2015-1067, DFN-CERT-2015-1038, DFN-CERT-2015-1016, DFN-CERT-2015-1012, DFN-CERT-2015-0980, DFN-CERT-2015-0977, DFN-CERT-2015-0976, DFN-CERT-2015-0960, DFN-CERT-2015-0956, DFN-CERT-2015-0944, DFN-CERT-2015-0937, DFN-CERT-2015-0925, DFN-CERT-2015-0884, DFN-CERT-2015-0881, DFN-CERT-2015-0879, DFN-CERT-2015-0866, DFN-CERT-2015-0844, DFN-CERT-2015-0800, DFN-CERT-2015-0737, DFN-CERT-2015-0696, DFN-CERT-2014-0977

Other: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1465_update_6.html
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 4.3) 22/tcp
NVT: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611)

Summary

The remote SSH server is configured to allow weak encryption algorithms.

Vulnerability Detection Result

The following weak client-to-server encryption algorithms are supported by the remote service:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

The following weak server-to-client encryption algorithms are supported by the remote service:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
arcfour
arcfour128
arcfour256
blowfish-cbc
cast128-cbc
rijndael-cbc@lysator.liu.se

Solution

Solution type: Mitigation

Disable the weak encryption algorithms.

Vulnerability Insight

The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.

The `none` algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.

A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.

Vulnerability Detection Method

Check if remote ssh service supports Arcfour, none or CBC ciphers.

Details: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611)

Version used: $Revision: 13568 $

References

Other: https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563

Medium (CVSS: 4.3) 80/tcp
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.801660)

Product detection result: cpe:/a:phpmyadmin:phpmyadmin:3.1.1 by phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

Summary

The host is running phpMyAdmin and is prone to Cross-Site Scripting Vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Solution

Solution type: WillNotFix

No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one.

Affected Software/OS

phpMyAdmin version 3.3.8.1 and prior.

Vulnerability Insight

The flaw is caused by input validation errors in the 'error.php' script when processing crafted BBcode tags containing '@' characters, which could allow attackers to inject arbitrary HTML code within the error page and conduct phishing attacks.

Vulnerability Detection Method

Details: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.801660)

Version used: $Revision: 11553 $

Product Detection Result

Product: cpe:/a:phpmyadmin:phpmyadmin:3.1.1
Method: phpMyAdmin Detection (OID: 1.3.6.1.4.1.25623.1.0.900129)

References

CVE: CVE-2010-4480
CERT: DFN-CERT-2011-0467, DFN-CERT-2011-0451, DFN-CERT-2011-0016, DFN-CERT-2011-0002
Other: http://www.exploit-db.com/exploits/15699/
http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 4.3) 80/tcp
NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

Summary

This host is running Apache HTTP Server and is prone to cookie information disclosure vulnerability.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow attackers to obtain sensitive information that may aid in further attacks.

Solution

Solution type: VendorFix

Upgrade to Apache HTTP Server version 2.2.22 or later.

Affected Software/OS

Apache HTTP Server versions 2.2.0 through 2.2.21

Vulnerability Insight

The flaw is due to an error within the default error response for status code 400 when no custom ErrorDocument is configured, which can be exploited to expose 'httpOnly' cookies.

Vulnerability Detection Method

Details: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.902830)

Version used: $Revision: 11857 $

References

CVE:	CVE-2012-0053
BID:	51706
CERT:	CB-K15/0080, CB-K14/1505, CB-K14/0608, DFN-CERT-2015-0082, DFN-CERT-2014-1592, DFN-CERT-2014-0635, DFN-CERT-2013-1307, DFN-CERT-2012-1276, DFN-CERT-2012-1112, DFN-CERT-2012-0928, DFN-CERT-2012-0758, DFN-CERT-2012-0744, DFN-CERT-2012-0568, DFN-CERT-2012-0425, DFN-CERT-2012-0424, DFN-CERT-2012-0387, DFN-CERT-2012-0343, DFN-CERT-2012-0332, DFN-CERT-2012-0306, DFN-CERT-2012-0264, DFN-CERT-2012-0203, DFN-CERT-2012-0188
Other:	http://secunia.com/advisories/47779
	http://www.exploit-db.com/exploits/18442
	http://rhn.redhat.com/errata/RHSA-2012-0128.html
	http://httpd.apache.org/security/vulnerabilities_22.html
	http://svn.apache.org/viewvc?view=revision&revision=1235454
	http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

Medium (CVSS: 4.0) 5432/tcp
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

The following certificates are part of the certificate chain but using insecure signature algorithms:

Subject:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
Signature Algorithm: sha1WithRSAEncryption

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)

- Message Digest 5 (MD5)

- Message Digest 4 (MD4)

- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1,Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Version used: $Revision: 8810 $

References

Other: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Medium (CVSS: 4.0) 25/tcp
NVT: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Summary

The remote service is using a SSL/TLS certificate in the certificate chain that has been signed using a cryptographically weak hashing algorithm.

Vulnerability Detection Result

The following certificates are part of the certificate chain but using insecure signature algorithms:

Subject:
1.2.840.113549.1.9.1=#726F6F74407562756E74753830342D626173652E6C6F63616C646F6D61696E,CN=ubuntu804-base.localdomain,OU=Office for Complication of Otherwise Simple Affairs,O=OCOSA,L=Everywhere,ST=There is no such thing outside US,C=XX
Signature Algorithm: sha1WithRSAEncryption

Solution

Solution type: Mitigation

Servers that use SSL/TLS certificates signed with a weak SHA-1, MD5, MD4 or MD2 hashing algorithm will need to obtain new SHA-2 signed SSL/TLS certificates to avoid web browser SSL/TLS certificate warnings.

Vulnerability Insight

The following hashing algorithms used for signing SSL/TLS certificates are considered cryptographically weak and not secure enough for ongoing use:

- Secure Hash Algorithm 1 (SHA-1)

- Message Digest 5 (MD5)

- Message Digest 4 (MD4)

- Message Digest 2 (MD2)

Beginning as late as January 2017 and as early as June 2016, browser developers such as Microsoft and Google will begin warning users when visiting web sites that use SHA-1 signed Secure Socket Layer (SSL) certificates.

NOTE: The script preference allows to set one or more custom SHA-1 fingerprints of CA certificates which are trusted by this routine. The fingerprints needs to be passed comma-separated and case-insensitive:

Fingerprint1

or

fingerprint1,Fingerprint2

Vulnerability Detection Method

Check which hashing algorithm was used to sign the remote SSL/TLS certificate.

Details: SSL/TLS: Certificate Signed Using A Weak Signature Algorithm (OID: 1.3.6.1.4.1.25623.1.0.105880)

Version used: $Revision: 8810 $

References

Other: https://blog.mozilla.org/security/2014/09/23/phasing-out-certificates-with-sha-1-based-signature-algorithms/

Medium (CVSS: 4.0) 5432/tcp
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 1024 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: $Revision: 12865 $

References

Other: https://weakdh.org/
https://weakdh.org/sysadmin.html

Medium (CVSS: 4.0) 25/tcp
NVT: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Summary

The SSL/TLS service uses Diffie-Hellman groups with insufficient strength (key size < 2048).

Vulnerability Detection Result

Server Temporary Key Size: 512 bits

Impact

An attacker might be able to decrypt the SSL/TLS communication offline.

Solution

Solution type: Workaround

Deploy (Ephemeral) Elliptic-Curve Diffie-Hellman (ECDHE) or use a 2048-bit or stronger Diffie-Hellman group (see the references).

For Apache Web Servers: Beginning with version 2.4.7, mod_ssl will use DH parameters which include primes with lengths of more than 1024 bits.

Vulnerability Insight

The Diffie-Hellman group are some big numbers that are used as base for the DH computations. They can be, and often are, fixed. The security of the final secret depends on the size of these parameters. It was found that 512 and 768 bits to be weak, 1024 bits to be breakable by really powerful attackers like governments.

Vulnerability Detection Method

Checks the DHE temporary public key size.

Details: SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerabili... (OID: 1.3.6.1.4.1.25623.1.0.106223)

Version used: $Revision: 12865 $

References

Other: https://weakdh.org/
https://weakdh.org/sysadmin.html

Low (CVSS: 3.5) 80/tcp
NVT: Tiki Wiki CMS Groupware XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.140797)

Product detection result: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5 by Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

Summary

An XSS vulnerability (via an SVG image) in Tiki allows an authenticated user to gain administrator privileges if an administrator opens a wiki page with a malicious SVG image, related to lib/filegals/filegallib.php.

Vulnerability Detection Result

Installed version: 1.9.5
Fixed version: 18.0

Solution

Solution type: VendorFix

Upgrade to version 18.0 or later.

Affected Software/OS

Tiki Wiki CMS Groupware prior to version 18.0.

Vulnerability Detection Method

Checks if a vulnerable version is present on the target host.

Details: Tiki Wiki CMS Groupware XSS Vulnerability (OID: 1.3.6.1.4.1.25623.1.0.140797)

Version used: $Revision: 12116 $

Product Detection Result

Product: cpe:/a:tiki:tikiwiki_cms/groupware:1.9.5
Method: Tiki Wiki CMS Groupware Version Detection (OID: 1.3.6.1.4.1.25623.1.0.901001)

References

CVE: CVE-2018-7188
Other: http://openwall.com/lists/oss-security/2018/02/16/1

Low (CVSS: 2.6) general/tcp
NVT: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Vulnerability Detection Result

It was detected that the host implements RFC1323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 65626
Packet 2: 65732

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution type: Mitigation

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See also: http://www.microsoft.com/en-us/download/details.aspx?id=9152

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

The remote host implements TCP timestamps, as defined by RFC1323.

Vulnerability Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details: TCP timestamps (OID: 1.3.6.1.4.1.25623.1.0.80091)

Version used: $Revision: 10411 $

References

Other: http://www.ietf.org/rfc/rfc1323.txt

Low (CVSS: 2.6) 22/tcp
NVT: SSH Weak MAC Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105610)

Summary

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

Vulnerability Detection Result

The following weak client-to-server MAC algorithms are supported by the remote service:

hmac-md5
hmac-md5-96
hmac-sha1-96

The following weak server-to-client MAC algorithms are supported by the remote service:

hmac-md5
hmac-md5-96
hmac-sha1-96

Solution

Solution type: Mitigation

Disable the weak MAC algorithms.

Vulnerability Detection Method

Details: SSH Weak MAC Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105610)

Version used: $Revision: 13568 $