Scan Report

September 11, 2024

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "scan01". The scan started at Wed Sep 11 15:57:08 2024 UTC and ended at Wed Sep 11 16:18:29 2024 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.19.130	11	9	2	0	0
Total: 1	11	9	2	0	0

Vendor security updates are not trusted.
Overrides are off. Even when a result has an override, this report uses the actual threat of the result.
Information on overrides is included in the report.
Notes are included in the report.
This report might not show details of all issues that were found.
Issues with the threat level "Log" are not shown.
Issues with the threat level "Debug" are not shown.
Issues with the threat level "False Positive" are not shown.
Only results with a minimum QoD of 70 are shown.

This report contains all 22 results selected by the filtering described above. Before filtering there were 217 results.

1.1 Host Authentications

Host	Protocol	Result	Port/User
192.168.19.130	SMB	Success	Protocol SMB, Port 445, User

2 Results per Host

2.1 192.168.19.130

Host scan start Wed Sep 11 15:57:40 2024 UTC
Host scan end Wed Sep 11 16:18:26 2024 UTC

Service (Port)	Threat Level
5432/tcp	High
80/tcp	High
general/tcp	High
21/tcp	High
513/tcp	High
3306/tcp	High
3632/tcp	High
6697/tcp	High
1524/tcp	High

. . . (continues) . . .

... (continued) ...

Service (Port)	Threat Level
6200/tcp	High
5432/tcp	Medium
80/tcp	Medium
25/tcp	Medium
general/icmp	Low
general/tcp	Low

2.1.1 High 5432/tcp

High (CVSS: 9.0)

NVT: PostgreSQL Default Credentials (PostgreSQL Protocol)

Product detection result
`cpe:/a:postgresql:postgresql:8.3.1`
`Detected by PostgreSQL Detection Consolidation (OID: 1.3.6.1.4.1.25623.1.0.12802`
`↪5)`

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

Quality of Detection (QoD): 99%

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 Default Credentials (PostgreSQL Protocol)`
OID:1.3.6.1.4.1.25623.1.0.103552
Version used: `2024-07-19T15:39:06Z`

Product Detection Result
Product: `cpe:/a:postgresql:postgresql:8.3.1`
Method: `PostgreSQL Detection Consolidation`
OID: 1.3.6.1.4.1.25623.1.0.128025)

[return to 192.168.19.130]

2.1.2 High 80/tcp

High (CVSS: 10.0)

NVT: TWiki XSS and Command Execution Vulnerabilities

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

Quality of Detection (QoD): 80%

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: `2024-03-01T14:37:10Z`

References
`cve: CVE-2008-5304`
`cve: CVE-2008-5305`
`url: http://twiki.org/cgi-bin/view/Codev.SecurityAlert-CVE-2008-5304`
`url: http://www.securityfocus.com/bid/32668`
`url: http://www.securityfocus.com/bid/32669`
`url: http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2008-5305`

High (CVSS: 9.8)

NVT: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check

Summary
PHP is prone to multiple vulnerabilities.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
By doing the following HTTP POST request:
"HTTP POST" body : <?php phpinfo();?>
URL              : http://192.168.19.130/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%7
↪5%72%6C%5F%69%6E%63%6C%75%64%65%3D%6F%6E+%2D%64+%73%61%66%65%5F%6D%6F%64%65%3D
↪%6F%66%66+%2D%64+%73%75%68%6F%73%69%6E%2E%73%69%6D%75%6C%61%74%69%6F%6E%3D%6F%
↪6E+%2D%64+%64%69%73%61%62%6C%65%5F%66%75%6E%63%74%69%6F%6E%73%3D%22%22+%2D%64+
↪%6F%70%65%6E%5F%62%61%73%65%64%69%72%3D%6E%6F%6E%65+%2D%64+%61%75%74%6F%5F%70%
↪72%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%6
↪3%67%69%2E%66%6F%72%63%65%5F%72%65%64%69%72%65%63%74%3D%30+%2D%64+%63%67%69%2E
↪%72%65%64%69%72%65%63%74%5F%73%74%61%74%75%73%5F%65%6E%76%3D%30+%2D%6E
it was possible to execute the "<?php phpinfo();?>" command.
Result:
  <title>phpinfo()</title><meta name="ROBOTS" content="NOINDEX,NOFOLLOW,NOARCHIV
↪E" /></head>
  <tr><td class="e">Configuration File (php.ini) Path </td><td class="v">/etc/ph
↪p5/cgi </td></tr>
  <h2>PHP Variables</h2>
```

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
Update to version 5.3.13, 5.4.3 or later.

Affected Software/OS
PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3.

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.

. . . continues on next page . . .

... continued from previous page ...

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

Vulnerability Detection Method
Send multiple a crafted HTTP POST requests and checks the responses.
This script checks for the presence of CVE-2012-1823 which indicates that the system is also vulnerable against the other included CVEs.
Details: PHP < 5.3.13, 5.4.x < 5.4.3 Multiple Vulnerabilities - Active Check
OID:1.3.6.1.4.1.25623.1.0.103482
Version used: 2024-07-17T05:05:38Z

References
cve: CVE-2012-1823
cve: CVE-2012-2311
cve: CVE-2012-2336
cve: CVE-2012-2335
url: https://web.archive.org/web/20190212080415/http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/
url: https://www.kb.cert.org/vuls/id/520827
url: https://bugs.php.net/bug.php?id=61910
url: https://www.php.net/manual/en/security.cgi-bin.php
url: https://web.archive.org/web/20210121223743/http://www.securityfocus.com/bid/53388
url: https://web.archive.org/web/20120709064615/http://www.h-online.com/open/news/item/Critical-open-hole-in-PHP-creates-risks-Update-2-1567532.html
url: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
cisa: Known Exploited Vulnerability (KEV) catalog

[return to 192.168.19.130]

2.1.3 High general/tcp

High (CVSS: 10.0)

NVT: Operating System (OS) End of Life (EOL) Detection

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

Summary

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 80%

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
```

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution:

Solution type: Mitigation

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

Vulnerability Detection Method

Checks if an EOL version of an OS is present on the target host.

Details: `Operating System (OS) End of Life (EOL) Detection`

OID:1.3.6.1.4.1.25623.1.0.103674

Version used: `2024-02-28T14:37:42Z`

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)

[return to 192.168.19.130]

2.1.4 High 21/tcp

High (CVSS: 9.8)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Product detection result

```
cpe:/a:beasts:vsftpd:2.3.4
Detected by vsFTPd FTP Server Detection (OID: 1.3.6.1.4.1.25623.1.0.111050)
```

... continues on next page ...

... continued from previous page ...

Summary
vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

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 vendor homepage. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method
Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `2023-12-07T05:05:41Z`

Product Detection Result
Product: `cpe:/a:beasts:vsftpd:2.3.4`
Method: `vsFTPd FTP Server Detection`
OID: 1.3.6.1.4.1.25623.1.0.111050)

References
`cve: CVE-2011-2523`
`url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd`
`↪oored.html`
`url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi`
`↪d/48539/`
`url: https://security.appspot.com/vsftpd.html`

[return to 192.168.19.130]

2.1.5 High 513/tcp

High (CVSS: 7.5)

NVT: The rlogin service is running

Summary
This remote host is running a rlogin service.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`The rlogin service is running on the target system.`

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: `The rlogin service is running`
OID:1.3.6.1.4.1.25623.1.0.901202
Version used: `2021-09-01T07:45:06Z`

References
`cve: CVE-1999-0651`

[return to 192.168.19.130]

2.1.6 High 3306/tcp

High (CVSS: 9.8)

NVT: MySQL / MariaDB Default Credentials (MySQL Protocol)

Product detection result
```
cpe:/a:mysql:mysql:5.0.51a
Detected by MariaDB / Oracle MySQL Detection (MySQL Protocol) (OID: 1.3.6.1.4.1.
↪25623.1.0.100152)
```

... continues on next page ...

... continued from previous page ...

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

Quality of Detection (QoD): 95%

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
- Contact the vendor for other possible fixes / updates

Affected Software/OS
The following products are know to use such weak credentials:
- CVE-2001-0645: Symantec/AXENT NetProwler 3.5.x
- CVE-2004-2357: Proofpoint Protection Server
- CVE-2006-1451: MySQL Manager in Apple Mac OS X 10.3.9 and 10.4.6
- CVE-2007-2554: Associated Press (AP) Newspower 4.0.1 and earlier
- CVE-2007-6081: AdventNet EventLog Analyzer build 4030
- CVE-2009-0919: XAMPP
- CVE-2014-3419: Infoblox NetMRI before 6.8.5
- CVE-2015-4669: Xsuite 2.x
- CVE-2016-6531, CVE-2018-15719: Open Dental before version 18.4

Other products might be affected as well.

Vulnerability Detection Method
Details: `MySQL / MariaDB Default Credentials (MySQL Protocol)`
OID:1.3.6.1.4.1.25623.1.0.103551
Version used: `2023-11-02T05:05:26Z`

Product Detection Result
Product: `cpe:/a:mysql:mysql:5.0.51a`
Method: `MariaDB / Oracle MySQL Detection (MySQL Protocol)`
OID: 1.3.6.1.4.1.25623.1.0.100152)

References
`cve: CVE-2001-0645`
`cve: CVE-2004-2357`
`cve: CVE-2006-1451`
`cve: CVE-2007-2554`
`cve: CVE-2007-6081`
`cve: CVE-2009-0919`
`cve: CVE-2014-3419`

... continues on next page ...

... continued from previous page ...

cve: CVE-2015-4669
cve: CVE-2016-6531
cve: CVE-2018-15719

[return to 192.168.19.130]

2.1.7 High 3632/tcp

High (CVSS: 9.3)

NVT: DistCC RCE Vulnerability (CVE-2004-2687)

Summary
DistCC is prone to a remote code execution (RCE) vulnerability.

Quality of Detection (QoD): 99%

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 Insight
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 Method
Details: DistCC RCE Vulnerability (CVE-2004-2687)
OID:1.3.6.1.4.1.25623.1.0.103553
Version used: 2022-07-07T10:16:06Z

References
cve: CVE-2004-2687
url: https://distcc.github.io/security.html
url: https://web.archive.org/web/20150511045306/http://archives.neohapsis.com:80

... continues on next page ...

... continued from previous page ...

↪/archives/bugtraq/2005-03/0183.html

[return to 192.168.19.130]

2.1.8 High 6697/tcp

High (CVSS: 7.5)

NVT: UnrealIRCd Backdoor

Summary
Detection of backdoor in UnrealIRCd.

Quality of Detection (QoD): 70%

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.

Affected Software/OS
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 Insight
Remote attackers can exploit this issue to execute arbitrary system commands within the context of the affected application.

Vulnerability Detection Method
Details: `UnrealIRCd Backdoor`
OID:1.3.6.1.4.1.25623.1.0.80111
Version used: `2023-08-01T13:29:10Z`

References
`cve: CVE-2010-2075`
`url: http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt`
`url: http://seclists.org/fulldisclosure/2010/Jun/277`
`url: http://www.securityfocus.com/bid/40820`

[return to 192.168.19.130]

2.1.9 High 1524/tcp

High (CVSS: 10.0)

NVT: Possible Backdoor: Ingreslock

Summary
A backdoor is installed on the remote host.

Quality of Detection (QoD): 99%

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
A whole cleanup of the infected system is recommended.

Vulnerability Detection Method
Details: `Possible Backdoor: Ingreslock`
OID:1.3.6.1.4.1.25623.1.0.103549
Version used: `2023-07-25T05:05:58Z`

[return to 192.168.19.130]

2.1.10 High 6200/tcp

High (CVSS: 9.8)

NVT: vsftpd Compromised Source Packages Backdoor Vulnerability

Summary
vsftpd is prone to a backdoor vulnerability.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

... continues on next page ...

... continued from previous page ...

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 vendor homepage. Please validate the package with its signature.

Affected Software/OS
The vsftpd 2.3.4 source package downloaded between 20110630 and 20110703 is affected.

Vulnerability Insight
The tainted source package contains a backdoor which opens a shell on port 6200/tcp.

Vulnerability Detection Method
Details: `vsftpd Compromised Source Packages Backdoor Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.103185
Version used: `2023-12-07T05:05:41Z`

References
`cve: CVE-2011-2523`
`url: https://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backd`
`↪oored.html`
`url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi`
`↪d/48539/`
`url: https://security.appspot.com/vsftpd.html`

[return to 192.168.19.130]

2.1.11 Medium 5432/tcp

Medium (CVSS: 5.9)

NVT: SSL/TLS: Report Weak Cipher Suites

Product detection result
`cpe:/a:ietf:transport_layer_security`
`Detected by SSL/TLS: Report Supported Cipher Suites (OID: 1.3.6.1.4.1.25623.1.0.`
`↪802067)`

Summary

... continues on next page ...

... continued from previous page ...

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.

Quality of Detection (QoD): 98%

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: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Report Supported Cipher Suites
OID: 1.3.6.1.4.1.25623.1.0.802067)

References
cve: CVE-2013-2566
cve: CVE-2015-2808
cve: CVE-2015-4000
url: https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k16-1
↪465_update_6.html
url: https://bettercrypto.org/

... continues on next page ...

... continued from previous page ...

url: https://mozilla.github.io/server-side-tls/ssl-config-generator/

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result

cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)

Summary

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result

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

fingerprint (SHA-1)	ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)	E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A ↪F1E32DEE436DE813CC
issued by	1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,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
public key algorithm	RSA
public key size (bits)	1024
serial	00FAF93A4C7FB6B9CC
signature algorithm	sha1WithRSAEncryption
subject	1.2.840.113549.1.9.1=#726F6F74407562756E747538 ↪30342D626173652E6C6F63616C646F6D61696E,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
valid from	2010-03-17 14:07:45 UTC
valid until	2010-04-16 14:07:45 UTC

Solution:

Solution type: Mitigation

Replace the SSL/TLS certificate by a new one.

Vulnerability Insight

... continues on next page ...

... continued from previous page ...

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: `2024-06-14T05:05:48Z`

Product Detection Result
Product: `cpe:/a:ietf:transport_layer_security`
Method: `SSL/TLS: Collect and Report Certificate Details`
OID: 1.3.6.1.4.1.25623.1.0.103692)

[return to 192.168.19.130]

2.1.12 Medium 80/tcp

Medium (CVSS: 6.8)

NVT: TWiki Cross-Site Request Forgery Vulnerability (Sep 2010)

Summary
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Quality of Detection (QoD): 80%

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

... continues on next page ...

... continued from previous page ...

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 (Sep 2010)`
OID:1.3.6.1.4.1.25623.1.0.801281
Version used: `2024-03-01T14:37:10Z`

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

Medium (CVSS: 6.0)

NVT: TWiki CSRF Vulnerability

Summary
TWiki is prone to a cross-site request forgery (CSRF) vulnerability.

Quality of Detection (QoD): 80%

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.

... continues on next page ...

... continued from previous page ...

Vulnerability Detection Method
Details: `TWiki CSRF Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.800400
Version used: `2024-06-28T05:05:33Z`

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

Medium (CVSS: 5.0)

NVT: awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result
`Vulnerable URL: http://192.168.19.130/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.

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 version 20100125 and prior.

Vulnerability Detection Method
Sends a crafted HTTP GET request and checks the response.
Details: `awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check`
OID:1.3.6.1.4.1.25623.1.0.103210
Version used: `2023-12-13T05:05:23Z`

... continues on next page ...

... continued from previous page ...

References
url: https://www.exploit-db.com/exploits/36047/
url: http://www.securityfocus.com/bid/49187

Medium (CVSS: 4.3)

NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Summary
phpMyAdmin is prone to a cross-site scripting (XSS) vulnerability.

Quality of Detection (QoD): 99%

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: 2023-10-17T05:05:34Z

References
cve: CVE-2010-4480
url: http://www.exploit-db.com/exploits/15699/
url: http://www.vupen.com/english/advisories/2010/3133

Medium (CVSS: 4.3)

NVT: Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Product detection result
cpe:/a:apache:http_server:2.2.8
Detected by Apache HTTP Server Detection Consolidation (OID: 1.3.6.1.4.1.25623.1
↪.0.117232)

Summary
Apache HTTP Server is prone to a cookie information disclosure vulnerability.

Quality of Detection (QoD): 99%

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
Update 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: 2022-04-27T12:01:52Z

Product Detection Result
Product: cpe:/a:apache:http_server:2.2.8
Method: Apache HTTP Server Detection Consolidation
OID: 1.3.6.1.4.1.25623.1.0.117232)

References
cve: CVE-2012-0053

. . . continues on next page . . .

... continued from previous page ...

url: http://secunia.com/advisories/47779
url: http://www.securityfocus.com/bid/51706
url: http://www.exploit-db.com/exploits/18442
url: http://rhn.redhat.com/errata/RHSA-2012-0128.html
url: http://httpd.apache.org/security/vulnerabilities_22.html
url: http://svn.apache.org/viewvc?view=revision&revision=1235454
url: http://lists.opensuse.org/opensuse-security-announce/2012-02/msg00026.html

[return to 192.168.19.130]

2.1.13 Medium 25/tcp

Medium (CVSS: 5.0)

NVT: Check if Mailserver answer to VRFY and EXPN requests

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

Quality of Detection (QoD): 99%

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: 2023-10-31T05:06:37Z

References
url: http://cr.yp.to/smtp/vrfy.html

Medium (CVSS: 5.0)

NVT: SSL/TLS: Certificate Expired

Product detection result

```
cpe:/a:ietf:transport_layer_security
Detected by SSL/TLS: Collect and Report Certificate Details (OID: 1.3.6.1.4.1.25
↪623.1.0.103692)
```

Summary

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

Quality of Detection (QoD): 99%

Vulnerability Detection Result

```
The certificate of the remote service expired on 2010-04-16 14:07:45.
Certificate details:
fingerprint (SHA-1)                | ED093088706603BFD5DC237399B498DA2D4D31C6
fingerprint (SHA-256)              | E7A7FA0D63E457C7C4A59B38B70849C6A70BDA6F830C7A
↪F1E32DEE436DE813CC
issued by                          | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,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
public key algorithm               | RSA
public key size (bits)             | 1024
serial                             | 00FAF93A4C7FB6B9CC
signature algorithm                | sha1WithRSAEncryption
subject                            | 1.2.840.113549.1.9.1=#726F6F74407562756E747538
↪30342D626173652E6C6F63616C646F6D61696E,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
valid from                         | 2010-03-17 14:07:45 UTC
valid until                        | 2010-04-16 14:07:45 UTC
```

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

. . . continues on next page . . .

... continued from previous page ...

Details: SSL/TLS: Certificate Expired
OID:1.3.6.1.4.1.25623.1.0.103955
Version used: 2024-06-14T05:05:48Z

Product Detection Result
Product: cpe:/a:ietf:transport_layer_security
Method: SSL/TLS: Collect and Report Certificate Details
OID: 1.3.6.1.4.1.25623.1.0.103692)

[return to 192.168.19.130]

2.1.14 Low general/icmp

Low (CVSS: 2.1)

NVT: ICMP Timestamp Reply Information Disclosure

Summary
The remote host responded to an ICMP timestamp request.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following response / ICMP packet has been received:
- ICMP Type: 14
- ICMP Code: 0

Impact
This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution:
Solution type: Mitigation
Various mitigations are possible:
- Disable the support for ICMP timestamp on the remote host completely
- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

Vulnerability Insight
The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Sends an ICMP Timestamp (Type 13) request and checks if a Timestamp Reply (Type 14) is received.
Details: ICMP Timestamp Reply Information Disclosure
OID:1.3.6.1.4.1.25623.1.0.103190
Version used: 2023-05-11T09:09:33Z

References
cve: CVE-1999-0524
url: https://datatracker.ietf.org/doc/html/rfc792
url: https://datatracker.ietf.org/doc/html/rfc2780

[return to 192.168.19.130]

2.1.15 Low general/tcp

Low (CVSS: 2.6)

NVT: TCP Timestamps Information Disclosure

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
It was detected that the host implements RFC1323/RFC7323.
The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 8728
Packet 2: 8836

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 the references for more information.

... continues on next page ...

... continued from previous page ...

Affected Software/OS
TCP implementations that implement RFC1323/RFC7323.

Vulnerability Insight
The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

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 Information Disclosure`
OID:1.3.6.1.4.1.25623.1.0.80091
Version used: `2023-12-15T16:10:08Z`

References
`url: https://datatracker.ietf.org/doc/html/rfc1323`
`url: https://datatracker.ietf.org/doc/html/rfc7323`
`url: https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/d`
`↪ownload/details.aspx?id=9152`
`url: https://www.fortiguard.com/psirt/FG-IR-16-090`

[return to 192.168.19.130]