Scan Report

October 31, 2025

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 "Black Box - Task". The scan started at Fri Oct 31 03:18:29 2025 UTC and ended at Fri Oct 31 04:07:36 2025 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
192.168.200.5	8	14	1	0	0
Total: 1	8	14	1	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 23 results selected by the filtering described above. Before filtering there were 282 results.

2 Results per Host

2.1 192.168.200.5

Host scan start	Fri Oct 31 03:24:29 2025 UTC
Host scan end	Fri Oct 31 04:07:28 2025 UTC

Service (Port)	Threat Level
6200/tcp	High
21/tcp	High
1524/tcp	High
5900/tcp	High
8787/tcp	High
80/tcp	High
21/tcp	Medium
5900/tcp	Medium
80/tcp	Medium
general/icmp	Low

2.1.1 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.

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 192.168.200.5]

2.1.2 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)`

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`

. . . continues on next page . . .

... continued from previous page ...

```
↪oored.html
url: https://web.archive.org/web/20210127090551/https://www.securityfocus.com/bi
↪d/48539/
url: https://security.appspot.com/vsftpd.html
```

High (CVSS: 7.5)

NVT: FTP Brute Force Logins With Default Credentials Reporting

Summary
It was possible to login into the remote FTP server using weak/known credentials.

Quality of Detection (QoD): 95%

Vulnerability Detection Result

```
It was possible to login with the following credentials <User>:<Password>
msfadmin:msfadmin
postgres:postgres
service:service
user:user
```

Impact
This issue may be exploited by a remote attacker to e.g. gain access to sensitive information or modify system configuration.

Solution:
Solution type: Mitigation
Change the password as soon as possible.

Vulnerability Insight
The following devices are / software is known to be affected:
- CVE-2001-1594: Codonics printer FTP service as used in GE Healthcare eNTEGRA P&R
- CVE-2013-7404: GE Healthcare Discovery NM 750b
- CVE-2014-9198: Schneider Electric ETG3000 FactoryCast HMI gateways
- CVE-2015-7261: QNAP iArtist Lite distributed with QNAP Signage Station
- CVE-2016-8731: Foscam C1 devices
- CVE-2017-8218: vsftpd on TP-Link C2 and C20i devices
- CVE-2018-9068: IMM2 for IBM and Lenovo System x
- CVE-2018-17771: Ingenico Telium 2 PoS terminals
- CVE-2018-19063, CVE-2018-19064: Foscam C2 and Opticam i5 devices

Note: As the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead.

Vulnerability Detection Method

... continues on next page ...

... continued from previous page ...

Reports weak/known credentials detected by the VT 'FTP Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108717).
Details: `FTP Brute Force Logins With Default Credentials Reporting`
OID:1.3.6.1.4.1.25623.1.0.108718
Version used: `2025-05-13T05:41:39Z`

References
`cve: CVE-1999-0501`
`cve: CVE-1999-0502`
`cve: CVE-1999-0507`
`cve: CVE-1999-0508`
`cve: CVE-2001-1594`
`cve: CVE-2013-7404`
`cve: CVE-2014-9198`
`cve: CVE-2015-7261`
`cve: CVE-2016-8731`
`cve: CVE-2017-8218`
`cve: CVE-2018-9068`
`cve: CVE-2018-17771`
`cve: CVE-2018-19063`
`cve: CVE-2018-19064`

[return to 192.168.200.5]

2.1.3 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

... continues on next page ...

... continued from previous page ...

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 192.168.200.5]

2.1.4 High 5900/tcp

High (CVSS: 9.0)

NVT: VNC Brute Force Login

Summary
Try to log in with given passwords via VNC protocol.

Quality of Detection (QoD): 95%

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: `2021-07-23T07:56:26Z`

[return to 192.168.200.5]

2.1.5 High 8787/tcp

High (CVSS: 10.0)

NVT: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities

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.

Quality of Detection (QoD): 99%

Vulnerability Detection Result
```
The service is running in $SAFE >= 1 mode. However it is still possible to run a
↪rbitrary syscall commands on the remote host. Sending an invalid syscall the s
↪ervice 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 `__se
↪nd__'"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 `m
↪ain_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:143
↪0:in `run'"1/usr/lib/ruby/1.8/drb/drb.rb:1427:in `start'"//usr/lib/ruby/1.8/dr
↪b/drb.rb:1427:in `run'"6/usr/lib/ruby/1.8/drb/drb.rb:1347:in `initialize'"//us
↪r/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 im
↪plemented
```

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.

. . . continues on next page . . .

... continued from previous page ...

Details: Distributed Ruby (dRuby/DRb) Multiple RCE Vulnerabilities
OID:1.3.6.1.4.1.25623.1.0.108010
Version used: 2024-06-28T05:05:33Z

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

[return to 192.168.200.5]

2.1.6 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.

... continues on next page ...

... continued from previous page ...

- %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://192.168.200.5/cgi-bin/php?%2D%64+%61%6C%6C%6F%77%5F%75
↪%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%6
↪E+%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%7
↪2%65%70%65%6E%64%5F%66%69%6C%65%3D%70%68%70%3A%2F%2F%69%6E%70%75%74+%2D%64+%63
↪%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

... continues on next page ...

... continued from previous page ...

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: Update to version 5.3.13, 5.4.3 or later
- Other products / applications: Please contact the vendor for a solution

Affected Software/OS
PHP versions prior to 5.3.13 and 5.4.x prior to 5.4.3.
Other products / applications might be affected by the tested CVE-2012-1823 as well.

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://example.com/index.php?-s

Vulnerability Detection Method
Send multiple a crafted HTTP POST requests and checks the responses.
Note: This script checks for the presence of CVE-2012-1823 which indicates that the system is also affected by 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: `2025-04-24T05:40:00Z`

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 192.168.200.5]

2.1.7 Medium 21/tcp

Medium (CVSS: 4.8)

NVT: FTP Unencrypted Cleartext Login

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Non-anonymous sessions: 331 Please specify the password.
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: `2023-12-20T05:05:58Z`

[return to 192.168.200.5]

2.1.8 Medium 5900/tcp

Medium (CVSS: 4.8)

NVT: VNC Server Unencrypted Data Transmission

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.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The VNC server provides the following insecure or cryptographically weak Securit
↪y 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: `2023-07-12T05:05:04Z`

References
`url: https://tools.ietf.org/html/rfc6143#page-10`

[return to 192.168.200.5]

2.1.9 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%

. . . continues on next page . . .

... continued from previous page ...

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 (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: 6.1)

NVT: TWiki < 6.1.0 XSS Vulnerability

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
Installed version: 01.Feb.2003
Fixed version: 6.1.0

... continues on next page ...

... continued from previous page ...

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: `2023-07-14T16:09:27Z`

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

Medium (CVSS: 6.1)

NVT: jQuery < 1.9.0 XSS Vulnerability

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.9.0
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.200.5/mutillidae/javascript/ddsmoothmenu/jquer
↪y.min.js
- Referenced at:   http://192.168.200.5/mutillidae/
```

Solution:
Solution type: VendorFix
Update to version 1.9.0 or later.

Affected Software/OS
jQuery prior to version 1.9.0.

... continues on next page ...

... continued from previous page ...

Vulnerability Insight
The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.9.0 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141636
Version used: `2023-07-14T05:06:08Z`

References
`cve: CVE-2012-6708`
`url: https://bugs.jquery.com/ticket/11290`
`cert-bund: WID-SEC-2022-0673`
`cert-bund: CB-K22/0045`
`cert-bund: CB-K18/1131`
`dfn-cert: DFN-CERT-2023-1197`

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

... continues on next page ...

... continued from previous page ...

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 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: 5.8)

NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

Summary
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.

Quality of Detection (QoD): 99%

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

... continues on next page ...

... continued from previous page ...

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
Checks if HTTP methods such as TRACE and TRACK are enabled and can be used.
Details: `HTTP Debugging Methods (TRACE/TRACK) Enabled`
OID:1.3.6.1.4.1.25623.1.0.11213
Version used: `2023-08-01T13:29:10Z`

References
`cve: CVE-2003-1567`
`cve: CVE-2004-2320`
`cve: CVE-2004-2763`
`cve: CVE-2005-3398`
`cve: CVE-2006-4683`
`cve: CVE-2007-3008`
`cve: CVE-2008-7253`
`cve: CVE-2009-2823`
`cve: CVE-2010-0386`
`cve: CVE-2012-2223`
`cve: CVE-2014-7883`
`url: http://www.kb.cert.org/vuls/id/288308`
`url: http://www.securityfocus.com/bid/11604`
`url: http://www.securityfocus.com/bid/15222`
`url: http://www.securityfocus.com/bid/19915`
`url: http://www.securityfocus.com/bid/24456`
`url: http://www.securityfocus.com/bid/33374`
`url: http://www.securityfocus.com/bid/36956`
`url: http://www.securityfocus.com/bid/36990`
`url: http://www.securityfocus.com/bid/37995`
`url: http://www.securityfocus.com/bid/9506`
`url: http://www.securityfocus.com/bid/9561`
`url: http://www.kb.cert.org/vuls/id/867593`
`url: https://httpd.apache.org/docs/current/en/mod/core.html#traceenable`
`url: https://techcommunity.microsoft.com/t5/iis-support-blog/http-track-and-trac`
`↪e-verbs/ba-p/784482`
`url: https://owasp.org/www-community/attacks/Cross_Site_Tracing`
`cert-bund: CB-K14/0981`

Medium (CVSS: 5.3)

NVT: phpinfo() Output Reporting (HTTP)

Summary

... continues on next page ...

... continued from previous page ...

Reporting of files containing the output of the phpinfo() PHP function previously detected via HTTP.

Quality of Detection (QoD): 80%

Vulnerability Detection Result

```
The following files are calling the function phpinfo() which disclose potentiall
↪y sensitive information:
http://192.168.200.5/mutillidae/phpinfo.php
Concluded from:
  <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>
http://192.168.200.5/phpinfo.php
Concluded from:
  <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

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.

Affected Software/OS

All systems exposing a file containing the output of the phpinfo() PHP function.
This VT is also reporting if an affected endpoint for the following products have been identified:
- CVE-2008-0149: TUTOS
- CVE-2023-49282, CVE-2023-49283: Microsoft Graph PHP SDK
- CVE-2024-10486: Google for WooCommerce plugin for WordPress

Vulnerability Insight

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 Method

... continues on next page ...

... continued from previous page ...

This script reports files identified by the following separate VT: 'phpinfo() Output Detection (HTTP)' (OID: 1.3.6.1.4.1.25623.1.0.108474).
Details: `phpinfo() Output Reporting (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.11229
Version used: `2025-07-09T05:43:50Z`

References
`cve: CVE-2008-0149`
`cve: CVE-2023-49282`
`cve: CVE-2023-49283`
`cve: CVE-2024-10486`
`url: https://www.php.net/manual/en/function.phpinfo.php`
`url: https://beaglesecurity.com/blog/vulnerability/revealing-phpinfo.html`

Medium (CVSS: 5.0)

NVT: /doc directory browsable

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.

Quality of Detection (QoD): 80%

Vulnerability Detection Result
`Vulnerable URL: http://192.168.200.5/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: `2023-08-01T13:29:10Z`

References
`cve: CVE-1999-0678`
`url: http://www.securityfocus.com/bid/318`

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://192.168.200.5/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: `2025-04-15T05:54:49Z`

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

Medium (CVSS: 5.0)

NVT: QWikiwiki directory traversal vulnerability

Summary
The remote host is running QWikiwiki, a Wiki application written in PHP.
The remote version of this software contains a validation input flaw which may allow an attacker to use it to read arbitrary files on the remote host with the privileges of the web server.

. . . continues on next page . . .

... continued from previous page ...

Quality of Detection (QoD): 99%

Vulnerability Detection Result
Vulnerable URL: http://192.168.200.5/mutillidae/index.php?page=../../../../../../../../../../etc/passwd%00

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.

Vulnerability Detection Method
Details: QWikiwiki directory traversal vulnerability
OID:1.3.6.1.4.1.25623.1.0.16100
Version used: 2025-04-15T05:54:49Z

References
cve: CVE-2005-0283
url: http://www.securityfocus.com/bid/12163

Medium (CVSS: 4.8)

NVT: Cleartext Transmission of Sensitive Information via HTTP

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
The following input fields were identified (URL:input name):
http://192.168.200.5/dvwa/login.php:password
http://192.168.200.5/phpMyAdmin/:pma_password
http://192.168.200.5/phpMyAdmin/?D=A:pma_password
http://192.168.200.5/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:

... continues on next page ...

... continued from previous page ...

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: `2023-09-07T05:05:21Z`

References
```
url: https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_Se
↪ssion_Management
url: https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
url: https://cwe.mitre.org/data/definitions/319.html
```

Medium (CVSS: 4.3)

NVT: jQuery < 1.6.3 XSS Vulnerability

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

Quality of Detection (QoD): 80%

Vulnerability Detection Result
```
Installed version: 1.3.2
Fixed version:     1.6.3
Installation
path / port:       /mutillidae/javascript/ddsmoothmenu/jquery.min.js
Detection info (see OID: 1.3.6.1.4.1.25623.1.0.150658 for more info):
- Identified file: http://192.168.200.5/mutillidae/javascript/ddsmoothmenu/jquer
↪y.min.js
- Referenced at:   http://192.168.200.5/mutillidae/
```

Solution:

... continues on next page ...

... continued from previous page ...

Solution type: VendorFix
Update to version 1.6.3 or later.

Affected Software/OS
jQuery prior to version 1.6.3.

Vulnerability Insight
Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.

Vulnerability Detection Method
Checks if a vulnerable version is present on the target host.
Details: `jQuery < 1.6.3 XSS Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141637
Version used: `2023-07-14T05:06:08Z`

References
`cve: CVE-2011-4969`
`url: https://blog.jquery.com/2011/09/01/jquery-1-6-3-released/`
`cert-bund: CB-K17/0195`
`dfn-cert: DFN-CERT-2016-0890`

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.

... continues on next page ...

... continued from previous page ...

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`

[return to 192.168.200.5]

2.1.10 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

... continues on next page ...

... continued from previous page ...

- 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
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: `2025-01-21T05:37:33Z`

References
`cve: CVE-1999-0524`
`url: https://datatracker.ietf.org/doc/html/rfc792`
`url: https://datatracker.ietf.org/doc/html/rfc2780`
`cert-bund: CB-K15/1514`
`cert-bund: CB-K14/0632`

[return to 192.168.200.5]