Scan Report

April 2, 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 "Assiignment". The scan started at Wed Apr 2 17:20:06 2025 UTC and ended at Wed Apr 2 17:26:02 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

Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.3.2	2	4	1	0	0
Total: 1	2	4	1	0	0

Vendor security updates are not trusted.
Overrides are on. When a result has an override, this report uses the threat of the override.
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.
It only lists hosts that produced issues.
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 7 results selected by the filtering described above. Before filtering there were 204 results.

Results per Host

192.168.3.2

Host scan start	Wed Apr 2 17:20:13 2025 UTC
Host scan end	Wed Apr 2 17:26:02 2025 UTC

Service (Port)	Threat Level
22/tcp	High
80/tcp	High
22/tcp	Medium
80/tcp	Medium
22/tcp	Low

High 22/tcp

High (CVSS: 7.5) NVT: Deprecated SSH-1 Protocol Detection
Summary The host is running SSH and is providing / accepting one or more deprecated versions of the SSH protocol which have known cryptograhic flaws.
. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result

```
The service is providing / accepting the following deprecated versions of the SS
↪H protocol which have known cryptograhic flaws:
1.33
1.5
```

Impact

Successful exploitation could allows remote attackers to bypass security restrictions and to obtain a client's public host key during a connection attempt and use it to open and authenticate an SSH session to another server with the same access.

Solution

Solution type: VendorFix

Reconfigure the SSH service to only provide / accept the SSH protocol version SSH-2.

Affected Software/OS

Services providing / accepting the SSH protocol version SSH-1 (1.33 and 1.5).

Vulnerability Detection Method

Details: `Deprecated SSH-1 Protocol Detection`
OID:1.3.6.1.4.1.25623.1.0.801993
Version used: `$Revision: 13586 $`

References

```
CVE: CVE-2001-0361, CVE-2001-0572, CVE-2001-1473
BID:2344
Other:
  URL:http://www.kb.cert.org/vuls/id/684820
   URL:http://xforce.iss.net/xforce/xfdb/6603
```

[return to 192.168.3.2]

High 80/tcp

High (CVSS: 7.5)
NVT: Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities

Product detection result

```
cpe:/a:secureideas:base:1.2.6
Detected by Basic Analysis and Security Engine Detection (OID: 1.3.6.1.4.1.25623
↪.1.0.100322)
```

Summary

... continues on next page ...

... continued from previous page ...

Basic Analysis and Security Engine (BASE) is prone to multiple input-validation vulnerabilities because it fails to adequately sanitize user-supplied input. These vulnerabilities include an SQL-injection issue, a cross-site scripting issue, and a local file-include issue.

Vulnerability Detection Result
`Installed version: 1.2.6`
`Fixed version: 1.4.4`

Impact
Exploiting these issues can allow an attacker to steal cookie-based authentication credentials, view and execute local files within the context of the webserver, compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. Other attacks may also be possible.

Solution
Solution type: VendorFix
Updates are available. Please see the references for details.

Affected Software/OS
These issues affect versions prior to BASE 1.4.4.

Vulnerability Detection Method
Details: `Basic Analysis and Security Engine Multiple Input Validation Vulnerabilities`
OID:1.3.6.1.4.1.25623.1.0.100323
Version used: `$Revision: 14031 $`

Product Detection Result
Product: `cpe:/a:secureideas:base:1.2.6`
Method: `Basic Analysis and Security Engine Detection`
OID: 1.3.6.1.4.1.25623.1.0.100322)

References
`CVE: CVE-2009-4590, CVE-2009-4591, CVE-2009-4592, CVE-2009-4837, CVE-2009-4838,`
`↪CVE-2009-4839`
`BID:36830, 18298`
`Other:`
`URL:http://www.securityfocus.com/bid/36830`
`URL:http://secureideas.sourceforge.net/`

[return to 192.168.3.2]

Medium 22/tcp

Medium (CVSS: 4.3)
NVT: SSH Weak Encryption Algorithms Supported

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 r
↪emote 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 r
↪emote 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`

. . . continues on next page . . .

... continued from previous page ...

OID:1.3.6.1.4.1.25623.1.0.105611
Version used: $Revision: 13581 $

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

[return to 192.168.3.2]

Medium 80/tcp

Medium (CVSS: 5.8)
NVT: HTTP Debugging Methods (TRACE/TRACK) Enabled

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,

... continues on next page ...

... continued from previous page ...

↪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
Other:
URL:http://www.kb.cert.org/vuls/id/288308
URL:http://www.kb.cert.org/vuls/id/867593
URL:http://httpd.apache.org/docs/current/de/mod/core.html#traceenable
URL:https://www.owasp.org/index.php/Cross_Site_Tracing

Medium (CVSS: 4.3)
NVT: phpMyAdmin 'error.php' Cross Site Scripting Vulnerability

Product detection result
cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Detected 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 $

... continues on next page ...

... continued from previous page ...

Product Detection Result
Product: cpe:/a:phpmyadmin:phpmyadmin:2.10.1
Method: phpMyAdmin Detection
OID: 1.3.6.1.4.1.25623.1.0.900129)

References
CVE: CVE-2010-4480
Other:
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

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
Other:

... continues on next page ...

... continued from previous page ...

```
  URL:http://secunia.com/advisories/47779
   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.htm
↪l
```

[return to 192.168.3.2]

Low 22/tcp

Low (CVSS: 2.6)
NVT: SSH Weak MAC Algorithms Supported

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 s
↪ervice:
hmac-md5
hmac-md5-96
hmac-sha1-96
The following weak server-to-client MAC algorithms are supported by the remote s
↪ervice:
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: 13581 $`

[return to 192.168.3.2]