Scan Report

November 19, 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 “game”. The scan started at Wed Nov 19 14:17:33 2025 UTC and ended at Wed Nov 19 14:35:37 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
10.10.10.129	1	5	1	0	0
Total: 1	1	5	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 45 results.

Results per Host

10.10.10.129

Host scan start	Wed Nov 19 14:18:05 2025 UTC
Host scan end	Wed Nov 19 14:35:37 2025 UTC

Service (Port)	Threat Level
10000/tcp	High
21/tcp	Medium
10000/tcp	Medium
general/tcp	Low

High 10000/tcp

High (CVSS: 7.5)
NVT: Webmin / Usermin Login Cross Site Scripting Vulnerability

Summary
This host is running Webmin/Usermin and is prone to cross site scripting vulnerability.

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

. . . continues on next page . . .

. . . continued from previous page . . .

Impact
Successful exploitation will allow remote attackers to insert arbitrary HTML and script code, which will be executed in a user's browser session in the context of an affected site.

Solution
Solution type: VendorFix
Upgrade to Webmin version 0.970, Usermin version 0.910 or later.

Affected Software/OS
Webmin version 0.96 and Usermin version 0.90

Vulnerability Insight
The flaw is due to improper validation of user-supplied input via the authentication page, which allows attackers to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

Vulnerability Detection Method
Details: `Webmin / Usermin Login Cross Site Scripting Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.802258
Version used: `$Revision: 12175 $`

References

```
CVE: CVE-2002-0756
BID:4694
Other:
  URL:http://xforce.iss.net/xforce/xfdb/9036
   URL:http://archives.neohapsis.com/archives/bugtraq/2002-05/0040.html
   URL:http://www.webmin.com/download.html
```

[return to 10.10.10.129]

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.

Vulnerability Detection Result

```
The remote FTP service accepts logins without a previous sent 'AUTH TLS' command
↪. Response(s):
Anonymous sessions:     331 User anonymous OK. Password required
Non-anonymous sessions: 331 User openvas-vt OK. Password required
```

. . . continues on next page . . .

... continued from previous page ...

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: 13611 $`

[return to 10.10.10.129]

Medium 10000/tcp

Medium (CVSS: 6.8)
NVT: Webmin <= 1.900 RCE Vulnerability

Product detection result

```
cpe:/a:webmin:webmin:1.590
Detected by Webmin / Usermin Detection (OID: 1.3.6.1.4.1.25623.1.0.10757)
```

Summary

Webmin is prone to an authenticate remote code execution vulnerability.

Vulnerability Detection Result

```
Installed version: 1.590
Fixed version:     None
```

Solution

Solution type: NoneAvailable

No known solution is available as of 08th March, 2019. Information regarding this issue will be updated once solution details are available.

Affected Software/OS

Webmin version 1.900 and probably prior.

Vulnerability Detection Method

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

... continues on next page ...

. . . continued from previous page . . .

Details: `Webmin <= 1.900 RCE Vulnerability`
OID:1.3.6.1.4.1.25623.1.0.141897
Version used: `$Revision: 14044 $`

Product Detection Result
Product: `cpe:/a:webmin:webmin:1.590`
Method: `Webmin / Usermin Detection`
OID: 1.3.6.1.4.1.25623.1.0.10757)

References

```
CVE: CVE-2019-9624
Other:
  URL:https://www.exploit-db.com/exploits/46201
```

Medium (CVSS: 5.0)
NVT: Webmin 1.880 Information Disclosure Vulnerability

Product detection result

```
cpe:/a:webmin:webmin:1.590
Detected by Webmin / Usermin Detection (OID: 1.3.6.1.4.1.25623.1.0.10757)
```

Summary
Webmin is prone to an information disclosure vulnerability that allows non-privileged users to access arbitrary files.

Vulnerability Detection Result

```
Installed version: 1.590
Fixed version:     Please see the solution tag for an available Mitigation
```

Impact
Successful exploitation would allow an attacker to access any file on the system, ranging from sensitive documents to administrator passwords.

Solution
Solution type: Mitigation
No patch is available as of 15th March, 2018. As a mitigation technique, the setting 'Can view any file as a log file' can be disabled, effectively stopping a user from exploiting this vulnerability.

Affected Software/OS
Webmin through version 1.880

Vulnerability Insight

. . . continues on next page . . .

. . . continued from previous page . . .

An issue was discovered in Webmin when the default Yes setting of 'Can view any file as a log file' is enabled. As a result of weak default configuration settings, limited users have full access rights to the underlying Unix system files, allowing the user to read sensitive data from the local system (using Local File Include) such as the '/etc/shadow' file via a 'GET /syslog/save_log.cgi?view=1&file=/etc/shadow' request.

Vulnerability Detection Method

The script checks if a vulnerable version is present on the target host.

Details: `Webmin 1.880 Information Disclosure Vulnerability`

OID:1.3.6.1.4.1.25623.1.0.113135

Version used: `$Revision: 12116 $`

Product Detection Result

Product: `cpe:/a:webmin:webmin:1.590`

Method: `Webmin / Usermin Detection`

OID: 1.3.6.1.4.1.25623.1.0.10757)

References

```
CVE: CVE-2018-8712
Other:
  URL:https://www.7elements.co.uk/resources/technical-advisories/webmin-1-840-1-
↪880-unrestricted-access-arbitrary-files-using-local-file-include/
   URL:http://www.webmin.com/changes.html
```

Medium (CVSS: 5.0)

NVT: Missing 'httpOnly' Cookie Attribute

Summary

The application is missing the 'httpOnly' cookie attribute

Vulnerability Detection Result

```
The cookies:
Set-Cookie: testing=***replaced***; path=/
are missing the "httpOnly" attribute.
```

Solution

Solution type: Mitigation

Set the 'httpOnly' attribute for any session cookie.

Affected Software/OS

Application with session handling in cookies.

Vulnerability Insight

The flaw is due to a cookie is not using the 'httpOnly' attribute. This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

. . . continues on next page . . .

. . . continued from previous page . . .

Vulnerability Detection Method

Check all cookies sent by the application for a missing 'httpOnly' attribute
Details: `Missing ‘httpOnly‘ Cookie Attribute`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `$Revision: 5270 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/HttpOnly
   URL:https://www.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-
↪002)
```

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.

Vulnerability Detection Result

```
The following input fields where identified (URL:input name):
http://10.10.10.129:10000/:pass
http://10.10.10.129:10000/unauthenticated:pass
```

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`

. . . continues on next page . . .

. . . continued from previous page . . .

OID:1.3.6.1.4.1.25623.1.0.108440
Version used: `$Revision: 10726 $`

References

```
Other:
  URL:https://www.owasp.org/index.php/Top_10_2013-A2-Broken_Authentication_and_S
↪ession_Management
   URL:https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure
   URL:https://cwe.mitre.org/data/definitions/319.html
```

[return to 10.10.10.129]

Low general/tcp

Low (CVSS: 2.6)
NVT: TCP timestamps

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: 50114
Packet 2: 50381
```

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.

Affected Software/OS

TCP/IPv4 implementations that implement RFC1323.

Vulnerability Insight

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

. . . continues on next page . . .

. . . continued from previous page . . .

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: 14310 $`

References

```
Other:
  URL:http://www.ietf.org/rfc/rfc1323.txt
   URL:http://www.microsoft.com/en-us/download/details.aspx?id=9152
```

[return to 10.10.10.129]