Scan Report

April 22, 2026

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Asia/Bangkok", which is abbreviated "+07". The task was "rdi-wp". The scan started at Mon Apr 20 16:38:03 2026 +07 and ended at Tue Apr 21 13:19:10 2026 +07. 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
104.21.6.120 rdi-wp.extremesofts.com	0	1	0	0	0
172.67.134.212 rdi-wp.extremesofts.com	0	1	1	0	0
Total: 2	0	2	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 3 results selected by the filtering described above. Before filtering there were 112 results.

2 Results per Host

2.1 104.21.6.120

Host scan start	Mon Apr 20 16:38:53 2026 +07
Host scan end	Tue Apr 21 13:08:44 2026 +07

Service (Port)	Threat Level
443/tcp	Medium

2.1.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

. . . continues on next page . . .

... continued from previous page ...

Vulnerability Detection Result
The cookie(s):
Set-Cookie: pll_language=en; expires=Tue, 20 Apr 2027 09:55:08 GMT; Max-Age=***r
↪eplaced***; path=/; secure; SameSite=Lax
is/are missing the "HttpOnly" cookie attribute.

Solution:
Solution type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Affected Software/OS
Any web application with session handling in cookies.

Vulnerability Insight
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: Missing 'HttpOnly' Cookie Attribute (HTTP)
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: 2024-01-12T23:12:12+07:00

References
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)

[return to 104.21.6.120]

2.2 172.67.134.212

Host scan start Mon Apr 20 16:38:53 2026 +07
Host scan end

Service (Port)	Threat Level
443/tcp	Medium
general/tcp	Low

2.2.1 Medium 443/tcp

Medium (CVSS: 5.0)
NVT: Missing 'HttpOnly' Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the 'HttpOnly' cookie attribute for one or more sent HTTP cookie.

Quality of Detection (QoD): 70%

Vulnerability Detection Result
```
The cookie(s):
Set-Cookie: pll_language=en; expires=Tue, 20 Apr 2027 09:41:54 GMT; Max-Age=***r
↪eplaced***; path=/; secure; SameSite=Lax
is/are missing the "HttpOnly" cookie attribute.
```

Solution:
Solution type: Mitigation
- Set the 'HttpOnly' cookie attribute for any session cookie
- Evaluate / do an own assessment of the security impact on the web server / application and create an override for this result if there is none (this can't be checked automatically by this VT)

Affected Software/OS
Any web application with session handling in cookies.

Vulnerability Insight
The flaw exists if a session cookie is not using the 'HttpOnly' cookie attribute.
This allows a cookie to be accessed by JavaScript which could lead to session hijacking attacks.

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application for a missing 'HttpOnly' cookie attribute.
Details: `Missing 'HttpOnly' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.105925
Version used: `2024-01-12T23:12:12+07:00`

References
```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.6
url: https://owasp.org/www-community/HttpOnly
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

[return to 172.67.134.212]

2.2.2 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: 4105284800
Packet 2: 4163999227
```

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 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: `2023-12-15T23:10:08+07:00`

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 172.67.134.212]
