Scan Report

February 27, 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 "Immediate scan of IP br.clover.com". The scan started at Wed Feb 12 05:47:24 2025 UTC and ended at Wed Feb 12 22:08:54 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
66.6.29.162 support.cardpointe.com	0	4	0	0	0
Total: 1	0	4	0	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 4 results selected by the filtering described above. Before filtering there were 106 results.

2 Results per Host

2.1 66.6.29.162

Host scan start	Wed Feb 12 05:49:04 2025 UTC
Host scan end	Wed Feb 12 22:08:43 2025 UTC

Service (Port)	Threat Level
443/tcp	Medium

2.1.1 Medium 443/tcp

Medium (CVSS: 5.0)

NVT: Missing ’Secure’ Cookie Attribute (HTTP)

Summary
The remote HTTP web server / application is missing to set the ’Secure’ 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: __uzma=6fe244ca-7bec-4203-8a0d-07c7c205030b; HttpOnly; path=/; Expir
↪es=Wed, 13-Aug-25 05:58:28 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmb=1739339908; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzme=5055; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28 GMT ;
↪ Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmc=992541095754; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:
↪28 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmd=1739339908; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:28
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
is/are missing the "Secure" cookie attribute.
```

Solution:

Solution type: Mitigation

- Set the ’Secure’ cookie attribute for any cookies that are sent over a SSL/TLS connection
- 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 accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

Vulnerability Insight

The flaw exists if a cookie is not using the ’Secure’ cookie attribute and is sent over a SSL/TLS connection.

This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

Vulnerability Detection Method

Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing ’Secure’ cookie attribute.

Details: `Missing ’Secure’ Cookie Attribute (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.902661

Version used: `2024-09-27T05:05:23Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
url: https://owasp.org/www-community/controls/SecureCookieAttribute
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

Medium (CVSS: 5.0)

NVT: Missing 'Secure' Cookie Attribute (HTTP)

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The cookie(s):
Set-Cookie: __uzma=199c00e6-3e8c-41b4-88c7-fac1c911b58a; HttpOnly; path=/; Expir
↪es=Wed, 13-Aug-25 10:40:22 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmb=1739356822; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:22
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzme=9063; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:22 GMT ;
↪ Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmc=513651043836; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:
↪22 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmd=1739356822; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:22
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
is/are missing the "Secure" cookie attribute.
```

Solution:
Solution type: Mitigation
- Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection
- 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 accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

Vulnerability Insight
The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.
This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

Vulnerability Detection Method
Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.
Details: `Missing 'Secure' Cookie Attribute (HTTP)`
OID:1.3.6.1.4.1.25623.1.0.902661
Version used: `2024-09-27T05:05:23Z`

. . . continues on next page . . .

. . . continued from previous page . . .

References

```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
url: https://owasp.org/www-community/controls/SecureCookieAttribute
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

Medium (CVSS: 5.0)

NVT: Missing 'Secure' Cookie Attribute (HTTP)

Summary

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The cookie(s):
Set-Cookie: __uzma=ed9e351c-25e2-425e-9706-9127c2980685; HttpOnly; path=/; Expir
↪es=Wed, 13-Aug-25 05:58:36 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmb=1739339916; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:36
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzme=1758; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:36 GMT ;
↪ Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmc=232181048201; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:
↪36 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmd=1739339916; HttpOnly; path=/; Expires=Wed, 13-Aug-25 05:58:36
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
is/are missing the "Secure" cookie attribute.
```

Solution:

Solution type: Mitigation

- Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection
- 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 accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

Vulnerability Insight

The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.

. . . continues on next page . . .

. . . continued from previous page . . .

This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

Vulnerability Detection Method

Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.

Details: `Missing 'Secure' Cookie Attribute (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.902661

Version used: `2024-09-27T05:05:23Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
url: https://owasp.org/www-community/controls/SecureCookieAttribute
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

Medium (CVSS: 5.0)

NVT: Missing 'Secure' Cookie Attribute (HTTP)

Summary

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

Quality of Detection (QoD): 70%

Vulnerability Detection Result

```
The cookie(s):
Set-Cookie: __uzma=6a3e79a4-9f0f-424e-8162-7ea285417b36; HttpOnly; path=/; Expir
↪es=Wed, 13-Aug-25 10:40:24 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmb=1739356824; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:24
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzme=2102; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:24 GMT ;
↪ Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmc=130671062359; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:
↪24 GMT ; Max-Age=***replaced***; SameSite=Lax
Set-Cookie: __uzmd=1739356824; HttpOnly; path=/; Expires=Wed, 13-Aug-25 10:40:24
↪ GMT ; Max-Age=***replaced***; SameSite=Lax
is/are missing the "Secure" cookie attribute.
```

Solution:

Solution type: Mitigation

- Set the 'Secure' cookie attribute for any cookies that are sent over a SSL/TLS connection
- 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)

. . . continues on next page . . .

. . . continued from previous page . . .

Affected Software/OS

Any web application accessible via a SSL/TLS connection (HTTPS) and at the same time also accessible over a cleartext connection (HTTP).

Vulnerability Insight

The flaw exists if a cookie is not using the 'Secure' cookie attribute and is sent over a SSL/TLS connection.

This allows a cookie to be passed to the server by the client over non-secure channels (HTTP) and subsequently allows an attacker to e.g. conduct session hijacking attacks.

Vulnerability Detection Method

Checks all cookies sent by the remote HTTP web server / application over a SSL/TLS connection for a missing 'Secure' cookie attribute.

Details: `Missing 'Secure' Cookie Attribute (HTTP)`

OID:1.3.6.1.4.1.25623.1.0.902661

Version used: `2024-09-27T05:05:23Z`

References

```
url: https://www.rfc-editor.org/rfc/rfc6265#section-5.2.5
url: https://owasp.org/www-community/controls/SecureCookieAttribute
url: https://wiki.owasp.org/index.php/Testing_for_cookies_attributes_(OTG-SESS-0
↪02)
```

[return to 66.6.29.162]