Hive Pro

Threat Level

Green

THREAT ADVISORY

VULNERABILITY REPORT

Drupal addresses a Guzzle third-party vulnerability

Date of Publication	Admiralty code	TA Number
14 June 2022	A1	TA2022116

Summary

The Drupal core project addresses security flaws in a third-party Guzzle library to handle HTTP requests and responses to external services. These may not directly affect Drupal core; however, it can have an impact on contributed projects or custom code on Drupal sites. Guzzle has found two vulnerabilities that have been rated high risk (as per the company)

CVEs

CVE	NAME	PATCH
CVE-2022-31042	Failure to strip the Cookie header on change in host or HTTP downgrade	✓
CVE-2022-31043	Fix failure to strip Authorization header on HTTP downgrade	✓

Technical Details

#1

The first vulnerability CVE-2022-31042 allows a remote attacker to gain access to sensitive information. This exists due to insecure implementation when handling HTTPS to HTTP redirects. This can cause the remote attacker to obtain an authentication cookie and compromise the affected applications. The second vulnerability CVE-2022-31043 also helps the attacker exploit information in a similar way.

#2

Guzzle users are encouraged to upgrade to the latest versions 6.5.7 or 7.4.4. as soon as possible. However, organizations using Drupal should upgrade to versions 9.4.0-rc2, 9.3.16 or 9.2.21

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-31042	Drupal: 9.2.0 - 9.2.20, 9.3.0 - 9.3.15, 9.4.0 rc1	cpe:2.3:a:drupal:drupal:9.4.0:rc1:*:*:*:*:*:*	CWE- 200
CVE-2022-31043	Guzzle: <=6.5.6 >=7.0.0,<=7.4.3	cpe:2.3:a:guzzlephp:guzzle:*:*:*:*:*:*:*:*	

Patch Links

https://www.drupal.org/project/drupal/releases/9.3.16

https://www.drupal.org/project/drupal/releases/9.2.21

https://www.drupal.org/project/drupal/releases/9.4.0-rc2

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/06/13/drupal-releases-security-updates

https://www.drupal.org/sa-core-2022-011

https://github.com/guzzle/guzzle/security/advisories/GHSA-f2wf-25xc-69c9

https://github.com/guzzle/guzzle/security/advisories/GHSA-w248-ffj2-4v5q

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

14 June 2022 • 3:07 AM

More at www.hivepro.com