computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

CERT-EU Security Advisory 2018-008

Drupal Core – Remote Code Execution

March 30, 2018 — v1.0

History:

- *30/03/2018 — v1.0: Initial publication*

Summary

Drupal is a content management system often used for Enterprise Content Management Projects. Drupal team announced a security advisory [5] for a vulnerability CVE-2018-7600 reported by Jasper Mattsson and rated as Highly Critical with a score of 21/25 based on the NIST Common Misuse Scoring System.

A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site.

Successful exploitation could lead to a potential compromise of the web application and possibly the underlying operating system as well.

Products Affected

This vulnerability affects the Drupal core and affects the 7.x, 8.3.x, 8.4.x, and 8.5.x versions of Drupal, for which the patches have been issued.

This vulnerability affects the Drupal core versions Drupal 8.2.x and earlier, as well as Drupal 6, however these versions will not be patched.

Recommendations

Upgrade to the most recent version of Drupal 7 or 8 core.

If you are running 7.x, upgrade to Drupal 7.58. If you are unable to upgrade immediately, you can attempt to apply the available patch [1] to fix the vulnerability until you are able to completely upgrade.

If you are running 8.5.x, upgrade to Drupal 8.5.1. If you are unable to upgrade immediately, you can attempt to apply the available patch [2] to fix the vulnerability until you are able to completely upgrade.

Drupal 8.3.x and 8.4.x are no longer supported and Drupal does not normally provide security releases for unsupported minor releases. However, given the potential severity of this issue, currently they are providing 8.3.x and 8.4.x releases that includes the fix for sites which have not yet had a chance to update to 8.5.0.

Your site's update report page will recommend the 8.5.x release even if you are on 8.3.x or 8.4.x. Consider to update to a supported version after installing this security update. If you are running 8.3.x, upgrade to Drupal 8.3.9 or apply the available patch [2]. If you are running 8.4.x, upgrade to Drupal 8.4.6 or apply the available patch [2].

This issue also affects Drupal 8.2.x and earlier, which are no longer supported. If you are running any of these versions of Drupal 8, update to a more recent release and then follow the instructions above.

This issue also affects Drupal 6. Drupal 6 is End-of-Life and will not be patched.

Mitigations

If you are unable to upgrade to Drupal 7.58 immediately, you can attempt to apply the available patch [1] to fix the vulnerability until upgrade to Drupal 7.58.

If you are unable to upgrade to Drupal 8.5.1, 8.3.9, or 8.4.6 immediately, you can attempt to apply the available patch [2] to fix the vulnerability until upgrade to non-vulnerable version of Drupal.

Exploits

Given that Drupal core is open source and diffs are available, we expect an exploit to be out soon [3, 4]. Drupal site owners must take action immediately or risk complete compromise of their web sites.

References

[1] https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=2266d2a83db50e2f97682d9a0fb8a18e2722cba5

[2] https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=5ac8738fa69df34a0635f0907d661b509ff9a28f

[3] https://security.berkeley.edu/news/highly-critical-remote-code-execution-drupal-sa-core-2018-002

[4] https://blog.appsecco.com/remote-code-execution-with-drupal-core-sa-core-2018-002-95e6ecc0c714

[5] https://www.drupal.org/sa-core-2018-002