CERT-EU Security Advisory 2018-012

Drupal Core – Remote Code Execution

April 27, 2018 — v1.0

History:

- *27/04/2018 — v1.0: Initial publication*

Summary

Drupal is a content management system often used for Enterprise Content Management Projects. A remote code execution vulnerability (CVE-2018-7602) [2] exists within multiple subsystems of Drupal 7.x and 8.x. This allows attackers to exploit multiple attack vectors on a Drupal site, which result in the site being compromised. This vulnerability is related to Drupal core - highly critical - Remote Code Execution - SA-CORE-2018-002 (CVE-2018-7600) [1, 8]. Both SA-CORE-2018-002/CERT-EU-SA2018-008 (CVE-2018-7600) and this vulnerability are being exploited in the wild.

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 7.59. [3]
- If you are running 8.5.x, upgrade to Drupal 8.5.3. [4]
- If you are running 8.4.x, upgrade to Drupal 8.4.8. [5]

Drupal 8.4.x is no longer supported and Drupal developers do not normally provide security releases for unsupported minor releases. However, in this case they are providing this 8.4.x release so that sites can update as quickly as possible. You should update to 8.4.8 immediately, then update to 8.5.3 or the latest secure release as soon as possible.

Workarounds

If you are unable to update immediately, or if you are running a Drupal distribution that does not yet include this security release, you can attempt to apply the patch below to fix the vulnerability until you are able to update completely:

IMPORTANT: These patches will only work if your site already has the fix from SA-CORE-2018-002 [1,8] applied. If your site does not have that fix, it may already be compromised!

- Patch for Drupal 8.x (8.5.x and below) [6]
- Patch for Drupal 7.x [7]

Exploits

This vulnerability is being exploited in the wild [2].

References

[1] https://cert.europa.eu/static/SecurityAdvisories/2018/CERT-EU-SA2018-008.pdf

[2] https://www.drupal.org/sa-core-2018-004

[3] https://www.drupal.org/project/drupal/releases/7.59

[4] https://www.drupal.org/project/drupal/releases/8.5.3

[5] https://www.drupal.org/project/drupal/releases/8.4.8

[6] https://cgit.drupalcode.org/drupal/rawdiff/?h=8.5.x&id=bb6d396609600d1169da29456ba3db59abae4b7e

[7] https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=080daa38f265ea28444c540832509a48861587d0

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