CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2019-005

Critical Flaw in Drupal Allows Remote Code Execution

February 26, 2019 — v1.1

TLP:WHITE

History:

- *22/02/2019 — v1.0 – Initial publication*
- *26/02/2019 — v1.1 – Additional exploit path*

Summary

An important security update was released by Drupal, which patches a remote code execution vulnerability (number CVE-2019-6340). The vulnerability was caused by the data passed into the RESTful Web service without strict verification. Successful exploitation of the vulnerability can result in remote code execution on the target host. RESTful services are not turned on by default, greatly reducing the risk of exploitation. For security reasons, users of Drupal are advised to upgrade in a timely manner [1, 2].

Technical Details

The vulnerability was caused by Drupal's lack of rigorous validation of RESTful Web data. If the site has a RESTful web service enabled and accepts PATCH, POST, or GET requests, or other web service modules enabled in the site, there will be a deserialization issue that will result in code execution [2, 3].

A site is affected by this if one of the following conditions is met:

- The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests [1]. According to [3] there is now also a new way to exploit this using GET requests as well.
- the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7.

Products Affected

- Drupal 8.6.9 and below
- Drupal 8.5.10 and below

Recommendations

- If you are using Drupal 8.6.x, upgrade to Drupal 8.6.10.
- If you are using Drupal 8.5.x, upgrade to Drupal 8.5.11.
- Be sure to install any available security updates for contributed projects after updating Drupal core.
- No core update is required for Drupal 7, but several Drupal 7 contributed modules do require updates.

Versions of Drupal 8 prior to 8.5.x are end-of-life and do not receive security coverage.

To immediately mitigate the vulnerability, you can disable all web services modules, or configure your web server(s) to not allow PUT/PATCH/POST requests to web services resources. Note that web services resources may be available on multiple paths depending on the configuration of your server(s). For Drupal 7, resources are for example typically available via paths (clean URLs) and via arguments to the `q` query argument. For Drupal 8, paths may still function when prefixed with `index.php/` [1].

References

[1] https://www.drupal.org/sa-core-2019-003

[2] https://meterpreter.org/cve-2019-6340-drupal-remote-code-execution/?cn-reloaded=1

[3] https://www.drupal.org/psa-2019-02-22