CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-038

Critical Wordpress Plugin Vulnerability

July 29, 2020 — v1.0

TLP:WHITE

History:

- *29/07/2020 — v1.0 – Initial publication*

Summary

On 19th of June, Wordfence Threat Intelligence team discovered a vulnerability that affects Wordpress plugin **Comments – wpDiscuz** [1]. This flaw gives unauthenticated attackers the ability to upload arbitrary files, including PHP files, and achieve remote code execution on a vulnerable site's server [1]. According to Wordfence, the security flaw is rated as critical severity with a CVSS base score of 10.0 [2].

Technical Details

Comments - wpDiscuz is a realtime comment system with custom comment form and fields. It is designed to supercharge WordPress native comments [3].

The wpDiscuz comments are intended to only allow image attachments [1]. However, due to the file MIME type detection functions that were used, the file type verification could easily be bypassed, allowing unauthenticated users the ability to upload any type of file, including PHP files [1]. Once uploaded to a vulnerable site's hosting server, attackers would get the file path location with the request's response making it easy to trigger file execution on the server and achieving remote code execution (RCE) [2].

Products Affected

The issue affects Wordpress plugin **Comments – wpDiscuz**, versions 7.0.0 - 7.0.4 [1].

Recommendations

The vulnerability was patched with the release of version 7.0.5 [1, 3].

CERT-EU recommends to update the vulnerable application as soon as possible.

References

[1] https://www.wordfence.com/blog/2020/07/critical-arbitrary-file-upload-vulnerability-patched-in-wpdiscuz-plugin/

[2] https://www.bleepingcomputer.com/news/security/critical-wordpress-plugin-bug-lets-hackers-take-over-hosting-account/

[3] https://wordpress.org/plugins/wpdiscuz/