Hive Pro

THREAT ADVISORY

Critical vulnerabilities found in WordPress plugin affecting 400,000 sites.

TA202123

Threat Level AMBER

Publish Date – July 8, 2021

Around 400,000 sites were affected by several critical vulnerabilities(CVE-2021-34621, CVE-2021-34622, CVE-2021-34623, CVE-2021-34624) discovered in ProfilePress, a WordPress plugin. The vulnerabilities are easily exploitable which makes it possible for an adversary to gain admin access and upload arbitrary files to vulnerable sites without requiring any prior authentication. The frequent exploitation of the WordPress plugin makes it important for targeted websites admin to update the plugin to the latest available patched version 3.1.4.

Vulnerability Details

CVE ID	Affected Versions	Vulnerability Name
CVE-2021-34621	3.0 – 3.1.3	Unauthenticated Privilege Escalation
CVE-2021-34622	3.0 – 3.1.3	Authenticated Privilege Escalation
CVE-2021-34623	3.0 – 3.1.3	Arbitrary File Upload in Image Uploader Component
CVE-2021-34624	3.0 – 3.1.3	Arbitrary File Upload in Image Uploader Component

References

https://www.wordfence.com/blog/2021/06/easily-exploitable-critical-vulnerabilities-patched-in-profilepress-plugin/
https://vulners.com/wpvulndb/WPVDB-ID:E12448EC-84A0-46AA-B280-5D9A80EE1E41