Hive Pro

THREAT ADVISORY

Millions of WordPress site backups at risk due to a vulnerability in UpdraftPlus plugin

TA2022039

Threat Level AMBER

Publish Date – Feb 21, 2022

UpdraftPlus is a backup tool for WordPress files, databases, plug-ins, and themes that allows you to create, restore, and migrate backups. UpdraftPlus is utilized by more than three million WordPress websites, according to its website, including those from P&G, NBA, Microsoft and NASA. An access control bypass vulnerability has been identified that allows even individuals with subscriber-level capabilities to access any UpdraftPlus backup.

An attacker can leverage this flaw to obtain access to privileged information stored in the database of the vulnerable site (e.g., usernames and hashed passwords).

This vulnerability has been fixed in UpdraftPlus Free version 1.22.3 & Premium version 2.22.3.

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
T1190: Exploit Public-Facing Application
TA0004: Privilege Escalation
T1068: Exploitation for Privilege Escalation

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0633	UpdraftPlus Free < 1.22.3 & Premium < 2.22.3	cpe:2.3:a:updraftplus:updraftplus:*:*:*:*:free:wordpress:*:*, cpe:2.3:a:updraftplus:updraftplus:*:*:*:*:premium:wordpress:*:*	WordPress UpdraftPlus Backup Disclosure Vulnerability	CWE-863

Patch Link

https://downloads.wordpress.org/plugin/updraftplus.1.22.4.zip
https://updraftplus.com/wp-content/uploads/updraftplus.zip

References

https://wpscan.com/vulnerability/d257c28f-3c7e-422b-a5c2-e618ed3c0bf3
https://jetpack.com/2022/02/17/severe-vulnerability-fixed-in-updraftplus-1-22-3/