Vulnerability in UpdraftPlus Plugin Exposed Millions of WordPress Site Backups

By Ionut Arghire on February 21, 2022

A high-severity vulnerability in the UpdraftPlus WordPress plugin can allow an attacker to obtain website backups that could contain sensitive information.

UpdraftPlus provides site administrators with backup and restoration capabilities, allowing them to store backups in the cloud and restore them with a click. The plugin has more than three million active installations.

On February 16, the plugin's developers released an update to address CVE-2022-0633 (CVSS score of 8.5), a security error that allows even users with subscriber-level permissions to access any backup that has been created with UpdraftPlus.

"This defect allows any logged-in user on a WordPress installation with UpdraftPlus active to exercise the privilege of downloading an existing backup, a privilege which should have been restricted to administrative users only," the UpdraftPlus development team notes.

The issue is related to a function that fails to ensure that a user sending a heartbeat request has administrator permissions. Thus, it allowed an attacker to craft a malicious request and retrieve information on the latest site backup, according to WordPress security and performance firm Jetpack, whose researchers discovered the flaw.

Site backups are securely identified using custom nonces and timestamps, and an attacker who is in the possession of these could access various plugin features, the researchers say.

[READ: Critical Code Execution Flaws Patched in 'PHP Everywhere' WordPress Plugin]

The researchers also discovered that, because the plugin did not properly validate user roles, even accounts with minimum privileges on the site could download backups and gain access to a site database.

Specifically, an attacker could abuse a feature in UpdraftPlus that allows for backup URLs to be sent to an email address set by the site owner, and have backup file URLs sent to email addresses the attacker controls.

The Wordfence team at WordPress security company Defiant says that, for an attack to be successful, the attacker needs to have an active account on the target system and they also needs to spoof the request to receive the URL via email, so as to appear it comes from a different endpoint.

“Affected sites are at risk of data loss / data theft via the attacker accessing a copy of your site’s backup, if your site contains anything non-public,” the UpdraftPlus team says.

The team also explains that, for the time being, no proof-of-concept (PoC) exploit code targeting the bug is available publicly, but warned that hackers could quickly reverse engineer the patch.

UpdraftPlus version 1.22.3, which patches the vulnerability, was released one day after the issue was reported to developers. Forced auto-updates have been pushed due to the severity of the flaw and a majority of plugin installations have already been updated to a patched version.

Related: Remote Code Execution Flaws Patched in WordPress Download Manager Plugin

Related: Actively Exploited Zero-Day Found in Popular WordPress eCommerce Plugin

Related: Vulnerability That Allows Complete WordPress Site Takeover Exploited in the Wild

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

CISA Warns Critical Infrastructure Organizations of Foreign Influence Operations
Vulnerability in UpdraftPlus Plugin Exposed Millions of WordPress Site Backups
Fast-Growing Golang-Based 'Kraken' Botnet Emerges
Microsoft Teams Abused for Malware Distribution in Recent Attacks
NSA Provides Guidance on Cisco Device Passwords

Tags:
NEWS & INDUSTRY Vulnerabilities