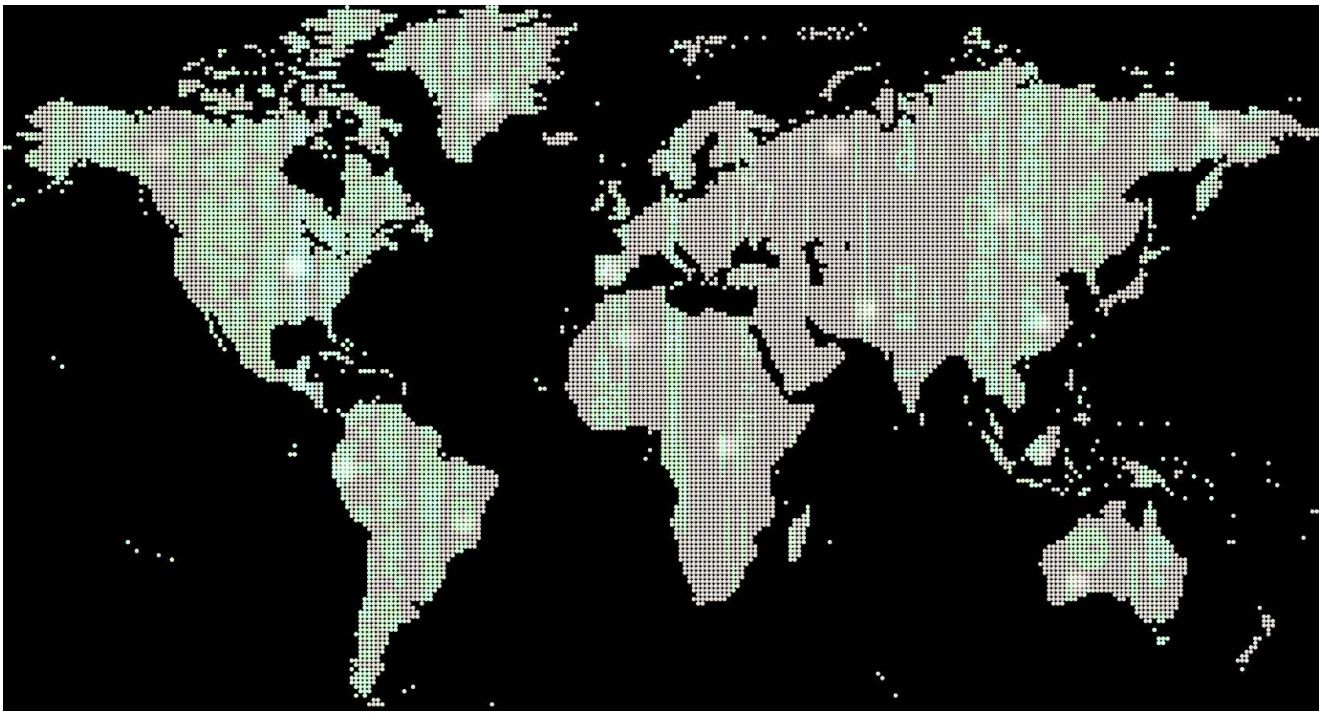
# Critical WordPress plugin zero-day under active exploitation

bleepingcomputer.com/news/security/critical-wordpress-plugin-zero-day-under-active-exploitation/

Sergiu Gatlan

By
Sergiu Gatlan

- June 1, 2021
- 01:25 PM
- 0



Threat actors are scanning for sites running the Fancy Product Designer plugin to exploit a zero-day bug allowing them to upload malware.

Fancy Product Designer is a visual product configurator plugin for WordPress, WooCommerce, and Shopify, and it allows customers to customize products using their own graphics and content.

According to sales statistics for the plugin, Fancy Product Designer has been sold and installed on more than 17,000 websites.

## Zero-day also impacts WooCommerce sites

Zero-days are publicly disclosed vulnerabilities vendors haven't patched, which, in some cases, are also actively exploited in the wild or have publicly available proof-of-concept exploits.

The security flaw is a critical severity remote code execution (RCE) vulnerability discovered by Wordfence security analyst Charles Sweethill on Monday.

"The WordPress version of the plugin is the one used in WooCommerce installations as well and is vulnerable," threat analyst Ram Gall told BleepingComputer.

When it comes to the plugin's Shopify version, attacks would likely be blocked, given that Shopify uses stricter access controls for sites hosted and running on its platform.

## Vulnerable sites exposed to complete takeover

Attackers who successfully exploit the Fancy Product Designer bug can bypass built-in checks blocking malicious files uploading to deploy executable PHP files on sites where the plugin is installed.

This allows the threat actors to completely take over vulnerable sites following remote code execution attacks.

"This attacker appears to be targeting e-commerce sites and attempting to extract order information from site databases," Gall said.

"As this order information contains personally identifiable information from customers, site owners are in a particularly difficult position if they are still running vulnerable versions of this plugin as it risks the e-commerce merchant’s PCI-DSS compliance.

"Due to this vulnerability being actively attacked, we are publicly disclosing with minimal details even though it has not yet been patched in order to alert the community to take precautions to keep their sites protected."

While the vulnerability has only been exploited on a small scale, the attacks targeting the thousands of sites running the Fancy Product Designer plugin have started more than four months ago, on January 30, 2021.

## Security update available

Since the vulnerability is under active exploitation and was rated as critical severity, customers are advised to immediately install the Fancy Product Designer 4.6.9 patched version released on June 2.

WordFence is still holding off on releasing additional details about this vulnerability until more sites running Fancy Product Designer update to the latest version given that the zero-day can be exploited "in some configurations" even after deactivation/

Detailed info on how to update the plugin (which doesn't come with an automatic update mechanism) and indicators of compromise, including IP addresses used to launch these ongoing attacks, are available in the WordFence report.

The Fancy Product Designer development team did not reply to BleepingComputer's request for comment before the article was published.

*Update: Added info on patched version released on June 2, 2021.*

## Related Articles:

Hackers target Tatsu WordPress plugin in millions of attacks

Critical flaw in Elementor WordPress plugin may affect 500k sites

Backdoor baked into premium school management plugin for WordPress

Critical Jupiter WordPress plugin flaws let hackers take over sites

Zyxel fixes firewall flaws that could lead to hacked networks