Critical 0-day in Fancy Product Designer Under Active Attack

wordfence.com/blog/2021/06/critical-0-day-in-fancy-product-designer-under-active-attack/

June 1, 2021

Update: A patched version of Fancy Product Designer, 4.6.9, is now available as of June 2, 2021. This article has been updated to reflect newly available information, including Indicators of Compromise.

On May 31, 2021, the Wordfence Threat Intelligence team discovered a critical file upload vulnerability being actively exploited in Fancy Product Designer, a WordPress plugin installed on over 17,000 sites.
We initiated contact with the plugin's developer the same day and received a response within 24 hours. We sent over the full disclosure the same day we received a response, on June 1, 2021. Due to this vulnerability being actively attacked, we are publicly disclosing with minimal details until users have time to update to the patched version in order to alert the community to take precautions to keep their sites protected.

While the Wordfence Firewall's built-in file upload protection sufficiently blocks the majority of attacks against this vulnerability, we determined that a bypass was possible in some configurations. As such, we released a new firewall rule to our premium customers on May 31, 2021. Sites still running the free version of Wordfence will receive the rule after 30 days, on June 30, 2021.

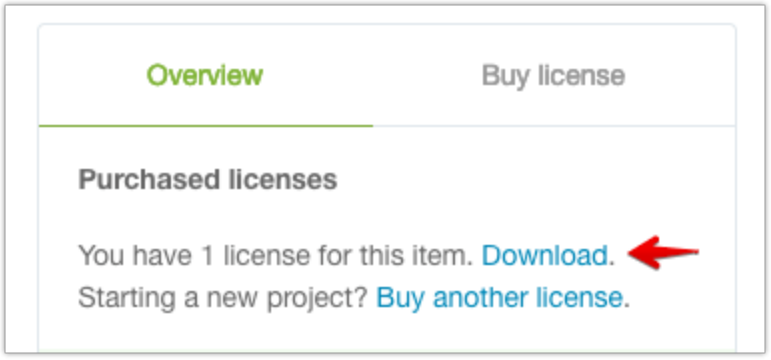
As this is a Critical 0-day under active attack and is exploitable in some configurations even if the plugin has been deactivated, we urge anyone using this plugin to update to the latest version available, 4.6.9, immediately.

Description: Unauthenticated Arbitrary File Upload and Remote Code Execution
Affected Plugin: Fancy Product Designer
Plugin Slug: fancy-product-designer
Affected Versions: < 4.6.9
CVE ID: CVE-2021-24370
CVSS Score: 9.8 (Critical)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Researcher/s: Charles Sweethill/Ram Gall
Fully Patched Version: 4.6.9
Fancy Product Designer is a WordPress plugin that offers the ability for customers to upload images and PDF files to be added to products. Unfortunately, while the plugin had some checks in place to prevent malicious files from being uploaded, these checks were insufficient and could easily be bypassed, allowing attackers to upload executable PHP files to any site with the plugin installed. This effectively made it possible for any attacker to achieve Remote Code Execution on an impacted site, allowing full site takeover.

We will provide a more detailed technical explanation of the vulnerability once more users have updated to a patched version.

How do I update?

In most cases you will need to login to codecanyon.net. Once you are logged in, you should be able to visit the product page at https://codecanyon.net/item/fancy-product-designer-woocommercewordpress/6318393. In the Overview sidebar on the right-hand side of the product page you should see a Download link:



Once you have downloaded the patched version of the plugin, you should be able to login to your WordPress site and go to Plugins->Add New->Upload Plugin to upload the patched plugin.

Indicators of Compromise

In most cases a successful attack results in a number of files which will appear in a subfolder of either
`wp-admin`
or
`wp-content/plugins/fancy-product-designer/inc`
with the date the file was uploaded. For instance:

`wp-content/plugins/fancy-product-designer/inc/2021/05/30/4fa00001c720b30102987d980e62d5e4.php`

or

`wp-admin/2021/05/31/4fa00001c720b30102987d980e62d5e4.php`

Update – the filenames in question are deterministic and we have added filenames associated with this vulnerability.
The following filenames and MD5 hashes are associated with this attack:

`ass.php` – MD5 `3783701c82396cc96d842839a291e813`. This is the initial payload, a dropper that then retrieves additional malware from a 3rd party site.
`op.php` – MD5 `29da9e97d5efe5c9a8680c7066bb2840`. A password-protected Webshell.
`prosettings.php` – MD5 `e6b9197ecdc61125a4e502a5af7cecae`. A Webshell found in older infections.
`4fa00001c720b30102987d980e62d5e4.php` – MD5 `4329689c76ccddd1d2f4ee7fef3dab71`. This payload decodes and loads a separate Webshell.
`4fa00001c720b30002987d983e62d5e1.jpg` – MD5 `c8757b55fc7d456a7a1a1aa024398471`. The compressed webshell loaded by `4fa00001c720b30102987d980e62d5e4.php`. Cannot be executed without the loader script.

The majority of attacks against this vulnerability are coming from the following IP addresses:

`69.12.71.82`
`92.53.124.123`
`46.53.253.152`

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

Our research indicates that this vulnerability is likely not being attacked on a large scale but has been exploited since at least May 16, 2021. *Update: Our Threat Intelligence Team has now found evidence of this vulnerability being exploited as early as January 30, 2021.*

Timeline

May 31, 2021 15:05 UTC – Wordfence Security Analyst Charles Sweethill finds evidence of a previously unknown vulnerability during malware removal and forensic investigation as part of a site cleaning and begins investigating possible attack vectors.
May 31, 2021 15:45 UTC – Charles notifies the Wordfence Threat Intelligence team and a full investigation begins.
May 31, 2021 16:20 UTC – We develop an initial proof of concept and begin work on a firewall rule.
May 31, 2021 17:06 UTC – We initiate contact with the plugin developer.
May 31, 2021 18:59 UTC – We release the firewall rule protecting against this vulnerability to Wordfence Premium customers.
June 1, 2021 09:03 UTC – The plugin developer responds to our initial contact.
June 1, 2021 13:35 UTC – We send over full disclosure.
June 2, 2021 – The plugin developer releases a patched version, 4.6.9, of the plugin.
June 30, 2021 – Firewall rule becomes available to free Wordfence users.

Conclusion

In today's article, we covered a critical 0-day vulnerability in Fancy Product Designer that is being actively attacked and used to upload malware onto sites that have the plugin installed.

While Wordfence Premium users should be protected against this vulnerability, we urge any users of this plugin to update to the latest version of the plugin, 4.6.9, immediately, as it is possible in some configurations to exploit the vulnerability even if the plugin is deactivated.

We will continue to monitor the situation and follow up as more information becomes available.

Special Thanks to Wordfence Security Analyst Charles Sweethill for discovering the vulnerability, determining the most likely vectors and indicators of compromise, and testing the firewall rule during a holiday. We also wanted to extend kudos the the plugin developer, radykal for quickly developing a patch for this issue.