

## XSS Vulnerability in NextScripts: Social Networks Auto-Poster Plugin Impacts 100,000 Sites

Note: To receive disclosures like this in your inbox the moment they're published, you can subscribe to our WordPress Security Mailing List.

On August 19, 2021, the Wordfence Threat Intelligence team began the disclosure process for a reflected Cross-Site Scripting(XSS) unlerability we found in <u>NextScripts: Social Networks Auto-Poster</u>, a WordPress plugin with over 100,000 installations.

The plugin's developer responded, so we confidentially provided the full disclosure the next day, on August 20, 2021. After several weeks without updates, we followed up with the developer on September 27, 2021, and a patched version of the plugin, 4.3.21, was released on October 4, 2021.

All Wordfence users, including Wordfence Premium customers as well as those still using the free version of Wordfence, are protected against this vulnerability by our firewall's built-in cross-site scripting protection.

```
Description: Reflected Cross-Site Scripting(XSS)

Affected Plugin: NextScripts: Social Networks Auto-Poster Plugin Slug: social-networks-auto-poster-facebook-twitterg
Affected Versions: < 4.3.20

CVE 10: (VE-2021-38356

CVS Score: 6. (Medium)

CVSS Vector: (VSS.3.1/AN/AGL/PRN/UIR/SC/CL/IL/J-AI
Researcherir: Ramuel Gall
Fully Patched Version: 4.3.21
```

The nxs\_ReposterListTable::column\_title function in inc/nxs\_class\_snap.php echoed out the value of \$\_REQUEST['page'] when an administrator was visiting the plugin administration page at wp-admin/admin.php?admin.php?page=nxssnap-post.

WordPress uses the value of the  $s_{\texttt{GET}}(\texttt{`page'})$  parameter in order to determine which administrative page to serve content for. It is also common practice for developers to use  $s_{\texttt{REQUEST}}$  for values stored in either  $s_{\texttt{GET}}$  or  $s_{\texttt{POST}}$ , as the  $s_{\texttt{REQUEST}}$  superglobal contains everything set in both  $s_{\texttt{GET}}$  and  $s_{\texttt{POST}}$ . As such,  $s_{\texttt{REQUEST}}(\texttt{`page'})$  might be expected to be set to the same value as  $s_{\texttt{GET}}(\texttt{`page'})$ .

However, thanks to a quirk of how PHP orders parameters that are present in multiple superglobal variables, it was possible to perform a reflected cross-site scripting attack.

In most PHP configurations, depending on the request\_order (or the variables\_order if request\_order is not set), spost takes precedence over s\_gst when populating s\_request. In other words, if both s\_gst('page') and s\_rost('page') are set, s\_request('page') will be set to the contents of s\_rost('page'), rather than s\_triangle(').

This meant that it was possible to execute JavaScript in the browser of a logged-in administrator by tricking them into visiting a self-submitting form that sent a Post request to their site, for example, hxxps://victimsite.site/wp-admin/admin.php?page-nxssnap-post, with the %\_Post ['page'] parameter set to malicious JavaScript.

The  $\$\_\texttt{GET}(`page')$  parameter could be set to nxssnap-post, so that WordPress would route the victim to the correct page, and then the malicious JavaScript in \$ post(`page') would be echoed out on that page.

As with all XSS attacks, malicious JavaScript running in an administrator's session could be used to add malicious administrative users or insert backdoors into a site, and thus be used for site takeover.

## Timeline

August 19, 2021 – We finish our investigation and begin the disclosure process for NextScripts: Social Networks Auto-

August 20, 2021 – We send over full disclosure to the plugin developer.

September 27, 2021 – We follow up with the plugin developer as the plugin has not yet been patched. October 4, 2021 – A patched version of the plugin, 4.3.21, becomes available.

## Conclusion

In today's post, we covered a reflected Cross-Site Scripting(XSS) vulnerability that relied on a relatively obscure quirk of how PHP handles superglobal variables.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as this is a serious vulnerability that can lead to complete site takeover.

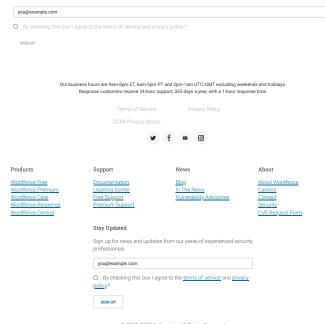
If your site has been compromised by an attack on this or any other plugin, our professional Site Cleaning services can help you get back in business.

Did you enjoy this post? Share it!

 $\textbf{All Wordfence users, including } \underline{\textbf{Wordfence Premium}} \ \textbf{customers and free Wordfence users are protected by our firewall's} \\$ 

## Breaking WordPress Security Research in your inbox as it happens.

Comments
No Comments



© 2012-2022 Defiant Inc. All Rights Reserved