NotificationX WordPress WooCommerce Plugin Vulnerabilities Impact 40k Sites via @sejournal, @martinibuster

A vulnerability advisory was published for the NotificationX FOMO plugin for WordPress and WooCommerce sites, affecting more than 40,000 websites. The vulnerability, which is rated at a 7.2 (High) severity level, enables unauthenticated attackers to inject malicious JavaScript that can execute in a visitor's browser when specific conditions are met.

NotificationX – FOMO Plugin

The NotificationX FOMO plugin is used by WordPress and WooCommerce site owners to display notification bars, popups, and real-time alerts such as recent sales, announcements, and promotional messages. The plugin is commonly deployed on marketing and e-commerce sites to create urgency and draw visitor attention through notifications.

Exposure Level

The vulnerability does not require any authentication or acquire any user role before launching an attack. Attackers do not need a WordPress account or any prior access to the site to trigger the vulnerability. Exploitation relies on getting a victim to visit a specially crafted page that interacts with the vulnerable site.

Root Cause Of The Vulnerability

The issue is a DOM-based Cross-Site Scripting (XSS) vulnerability tied to how the plugin processes preview data. In the context of a WordPress plugin vulnerability, DOM-based Cross-Site Scripting (XSS) vulnerability happens when a WordPress plugin contains client-side JavaScript that processes data from an untrusted source (the “source”) in an unsafe way, usually by writing the data to the web page (the “sink”).

In the context of the NotificationX plugin, the vulnerability exists because the plugin’s scripts accepts input through the nx-preview POST parameter, but does not properly sanitize the input or escape the output before it is rendered in the browser. Security checks that are supposed to check that user-supplied data is treated as plain text are missing. This allows an attacker to create a malicious web page that automatically submits a form to the victim’s site, forcing the victim’s browser to execute harmful scripts injected via that parameter.

The end result is that an attacker-controlled input can be interpreted as executable JavaScript instead of harmless preview content.

What Attackers Can Do

If exploited, the vulnerability enables attackers to execute arbitrary JavaScript in the context of the affected site. The injected script executes when a user visits a malicious page that automatically submits a form to the vulnerable NotificationX site.

This can allow attackers to:

- Hijack logged-in administrator or editor sessions
- Perform actions on behalf of authenticated users

- Redirect visitors to malicious or fraudulent websites
- Access sensitive information available through the browser

The official Wordfence advisory explains:

> *“The NotificationX – FOMO, Live Sales Notification, WooCommerce Sales Popup, GDPR, Social Proof, Announcement Banner & Floating Notification Bar plugin for WordPress is vulnerable to DOM-Based Cross-Site Scripting via the ‘nx-preview’ POST parameter in all versions up to, and including, 3.2.0. This is due to insufficient input sanitization and output escaping when processing preview data. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute when a user visits a malicious page that auto-submits a form to the vulnerable site.”*

Affected Versions

All versions of NotificationX up to and including 3.2.0 are vulnerable. A patch is available and the vulnerability was addressed in NotificationX version 3.2.1, which includes security enhancements related to this issue.

Recommended Action

Site owners using NotificationX are recommended to update their plugin immediately to version 3.2.1 or later. Sites that cannot update should disable the plugin until the patched version can be applied. Leaving vulnerable versions active exposes visitors and logged-in users to client-side attacks that can be difficult to detect and mitigate.

One More Vulnerability

This plugin has another vulnerability that is rated 4.3 medium threat level. The Wordfence advisory for this one describes it like this:

> *“The NotificationX plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ‘regenerate’ and ‘reset’ REST API endpoints in all versions up to, and including, 3.1.11. This makes it possible for authenticated attackers, with Contributor-level access and above, to reset analytics for any NotificationX campaign, regardless of ownership.”*

The NotificationX WordPress plugin includes two REST API endpoints called “regenerate” and “reset.” These endpoints are used to manage campaign analytics, such as resetting or rebuilding the stats that show how a notification is performing.

The problem is that these endpoints do not properly check user permissions for modifying data. In this case, the plugin only checks whether a user is logged in with Contributor-level access or higher, not whether they are actually allowed to perform the action. Even though users with the Contributor level role normally have very limited permissions, this flaw lets them perform actions they should not be able to do.

In this case, the damage that an attacker can do is limited. For example, an attacker can’t take over a site. Updated to version 3.2.1 or higher (same as the other vulnerability) will patch this vulnerability.

An attacker can:

- Reset analytics for any NotificationX campaign
- Do this even if they did not create or own the campaign
- Repeatedly wipe or regenerate campaign statistics

Featured Image by Shutterstock/Art Furnace

https://www.searchenginejournal.com/notificationx-wordpress-plugin-vulnerabilities/565510/