UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00241

WORDPRESS SITES EXPOSED BY INSECURE REST-API

DATE ISSUED: 25th January 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

A WordPress Email Template Designer used with WordPress sites - WP HTML Mail plugin, has been proven to be vulnerable to a Cross-Site Scripting (XSS) flaw which could allow attackers to inject malicious code, phishing scams and much more.

BREAKDOWN

An attacker can take advantage of faulty configuration in the REST-API routes and change settings without the need for authentication to access the endpoint. A malicious actor could then use this access to retrieve email theme settings, add new users, escalate privileges, and inject malicious code into the mail template that would be set to execute any time and administrator accesses the mail editor. Currently being tracked as CVE-2022-0218 with a CVSS criticality score of 8.3, this plugin is installed on 20,000 WordPress sites and is able to be integrated with other popular e-commerce platforms such as WooCommerce. Ninja forms and BuddyPress. Last week 3 other high-severity security warnings were also issued for WordPress sites – see Cyber Guidance Issue 0238 for more information

REMEDIATION STEPS

- Verify your WordPress site is updated and pathed to the latest version available (3.1 as at 21/01/2022)

REFERENCES & RESOURCES

ThreatPost https://threatpost.com/wordpress-insecure-plugin-rest-api/177866/
Wordfene https://www.wordfence.com/blog/2022/01/unauthenticated-xss-vulnerability-patched-in-html-email-template-designer-plugin/
WordPress https://wordpress.org/plugins/wp-html-mail/