UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0336

MULTIPLE FLAWS IN THE WORDPRESS NINJA PLUGIN

DATE ISSUED: 02nd August 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Numerous vulnerabilities have been discovered in the WordPress Ninja plugin that could be exploited by threat actors to escalate privileges and steal sensitive data.

BREAKDOWN

Security researchers at Patchstack have discovered three vulnerabilities in the popular form-building plugin Ninja Forms that could allow an attacker to gain administrative rights and steal user data. The first vulnerability tracked as CVE-2023-37979 is a post-based cross-site scripting (XSS) flaw that could allow an attacker to achieve privilege escalation and steal sensitive information by tricking users to visit a specially crafted webpage. CVE-2023-38386 and CVE-2023-38393 have broken access control flaws in the form submissions export feature that could allow attackers to transfer all Ninja Forms submissions on a WordPress site. These vulnerabilities affect Ninja Forms versions 3.6.25 and below. If a website allows membership and user registrations and is using a vulnerable version of the Ninja Forms plugin, it could be at high risk of experiencing a significant data breach incident due to this flaw.

REMEDIATION STEPS

- Update the Ninja Forms plugins to the latest version 3.6.26 to fix the vulnerabilities.
- Temporarily deactivate the plugin on the website until a patch is available and can be applied.
- Use complex and unique passwords for all user accounts, including administrators, editors, and contributors.
- Employ a Web Application Firewall (WAF) to protect your website from common security threats, including SQL injection and cross-site scripting (XSS) attacks.
- Practice the Principle of Least Privilege on all systems and services to lower the risk of attacks.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/wordpress-ninja-forms-plugin-flaw-lets-hackers-steal-submitted-data/
The Hacker News	https://thehackernews.com/2023/07/multiple-flaws-found-in-ninja-forms.html