CIRT.GY Guyana National Computer Incident Response Team

AL2024_04 Critical Security Flaws Discovered in WordPress Plugins - Urgent Action Required (March 26, 2024)

Description

WordPress users are urged to take immediate action following the discovery of critical security vulnerabilities in two popular plugins developed by miniOrange: Malware Scanner and Web Application Firewall. Tracked as CVE-2024-2172, the flaw affects Malware Scanner versions up to 4.7.2 and Web Application Firewall versions up to 2.1.1. With respective active installations of over 10,000 and 300, these plugins have been permanently closed by their maintainers as of March 7, 2024. The vulnerabilities allow unauthenticated attackers to gain administrative privileges, potentially leading to the complete compromise of affected WordPress sites.

Details

The vulnerability, discovered by Stiofan and reported by Wordfence, stems from a missing capability check in the function **mo_wpns_init()**. This oversight enables unauthenticated attackers to arbitrarily update any user's password, effectively granting themselves administrative privileges. Once administrative access is gained, attackers can manipulate site components, including uploading malicious plugin and theme files, modifying content to redirect users to malicious sites, or injecting spam content. With a CVSS score of 9.8 out of 10, the severity of this flaw underscores the urgent need for action.

In a similar vein, another high-severity privilege escalation flaw has been identified in the RegistrationMagic plugin (CVE-2024-1991, CVSS score: 8.8), affecting all versions up to 5.3.0.0. Authenticated attackers with subscriber-level permissions or higher can exploit this vulnerability to elevate their privileges to that of a site administrator, potentially leading to complete site compromise.

Remediation:

- **Immediate Removal:** WordPress users are strongly advised to delete the Malware Scanner and Web Application Firewall plugins from their websites without delay.
- **Update RegistrationMagic Plugin:** If you are using the RegistrationMagic plugin, update it to version 5.3.1.0 or later, released on March 11, 2024, to mitigate the privilege escalation vulnerability (CVE-2024-1991).
- **Regular Security Audits:** Conduct regular security audits of your WordPress site to detect any signs of compromise or suspicious activity.
- **Stay Informed:** Keep abreast of security advisories and updates from reputable sources to stay ahead of potential threats.

Taking these proactive measures is crucial to safeguarding your WordPress website from potential exploitation and ensuring the security and integrity of your online presence. Failure to act promptly may expose your site and its users to severe risks and compromise.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- The Hacker News. (2024, March 18). *WordPress admins urged to remove MiniOrange plugins due to critical flaw*. Retrieved from Hacker News. https://thehackernews.com/2024/03/wordpress-admins-urged-to-remove.html
- Divya. (2024, March 18). *Discontinued WordPress plugin flaw exposes websites to attacks*. GBHackers on Security | #1 Globally Trusted Cyber Security News Platform. https://gbhackers.com/discontinued-wordpress-plugin-flaw/#google_vignette