

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Critical Flaw In WordPress Plugins Poses Risk Of Site Takeover

Date of Publication

March 19, 2024

Admiralty Code

A1

TA Number

TA2024105




# Summary

**Discovered On:** March 2024

**Affected Products:** Malware Scanner and Web Application Firewall Plugins

**Impact:** A critical security vulnerability, identified as CVE-2024-2172 in WordPress, urges users utilizing miniOrange's Malware Scanner and Web Application Firewall plugins to uninstall these plugins from their websites. This vulnerability enables unauthorized attackers to gain administrative privileges by altering the user password.

## CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-2172	WordPress Privilege Escalation Vulnerability	Malware Scanner and Web Application Firewall Plugins			

# Vulnerability Details

## #1

A critical security vulnerability, tracked as CVE-2024-2172, in WordPress, urging users utilizing miniOrange's Malware Scanner and Web Application Firewall plugins to uninstall them from their websites. The Web Application Firewall plugin has been installed on over 300 websites, while the Malware Scanner plugin has been installed on more than 10,000 websites.

## #2

The MiniOrange WordPress plugins, including Malware Scanner and Web Application Firewall, are vulnerable to privilege escalation due to the absence of a capability check in the `mo_wpns_init()` function. This vulnerability allows unauthorized attackers to elevate their privileges to administrator level.

## #3

The problem stems from the `handle_change_password()` method's improper handling of the function `wp_authenticate_username_password()`, which is called when the plugin adds the `mo_wpns_init()` function to the init hook. This vulnerability makes it possible for unauthorised users to alter any user's password, raising the possibility of privilege escalation and potential site compromise.

## #4

Exploiting this vulnerability, attackers can manipulate posts and pages, upload malicious plugin and theme files, redirect visitors to malicious websites, or inject spam content into the targeted website. An updated version for both the plugins has been released which removes init hook for `mo_wpns_init()`. However, Users are advised to remove these two plugins, as they are no longer supported.

## Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-2172	Malware Scanner: Versions <= 4.7.2, Web Application Firewall: Versions <= 2.1.1	cpe:2.3:a:wordpress:MalwareScanner:*:*:*:*:* cpe:2.3:a:wordpress:WebApplicationFirewall:*:*:*:*:*	CWE-280

## Recommendations



**Remove Plugins:** Administrators should uninstall the miniOrange Malware Scanner and Web Application Firewall plugins. Both plugins have reached their End of Life and are no longer maintained.



**Log Analysis:** Implement thorough system monitoring practices and employ advanced log analysis techniques to detect any unauthorized modifications to the system. This includes closely monitoring activities such as password changes, new plugin uploads, and alterations to system files. By scrutinizing logs for unusual or suspicious activities, potential security threats can be identified and addressed promptly, helping to maintain the integrity and security of the system.



**Vulnerability Management:** Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

## Potential MITRE ATT&CK TTPs

<b><u>TA0042</u></b> Resource Development	<b><u>TA0001</u></b> Initial Access	<b><u>TA0004</u></b> Privilege Escalation	<b><u>TA0006</u></b> Credential Access
<b><u>T1588</u></b> Obtain Capabilities	<b><u>T1588.006</u></b> Vulnerabilities	<b><u>T1190</u></b> Exploit Public-Facing Application	<b><u>T1068</u></b> Exploitation for Privilege Escalation
<b><u>T1212</u></b> Exploitation for Credential Access			

## Patch Details

Both the plugins has been updated with an upgraded version that removes the `mo_wpns_init()` init hook. However, it is recommended that users uninstall these two plugins as they are no longer maintained and supported.

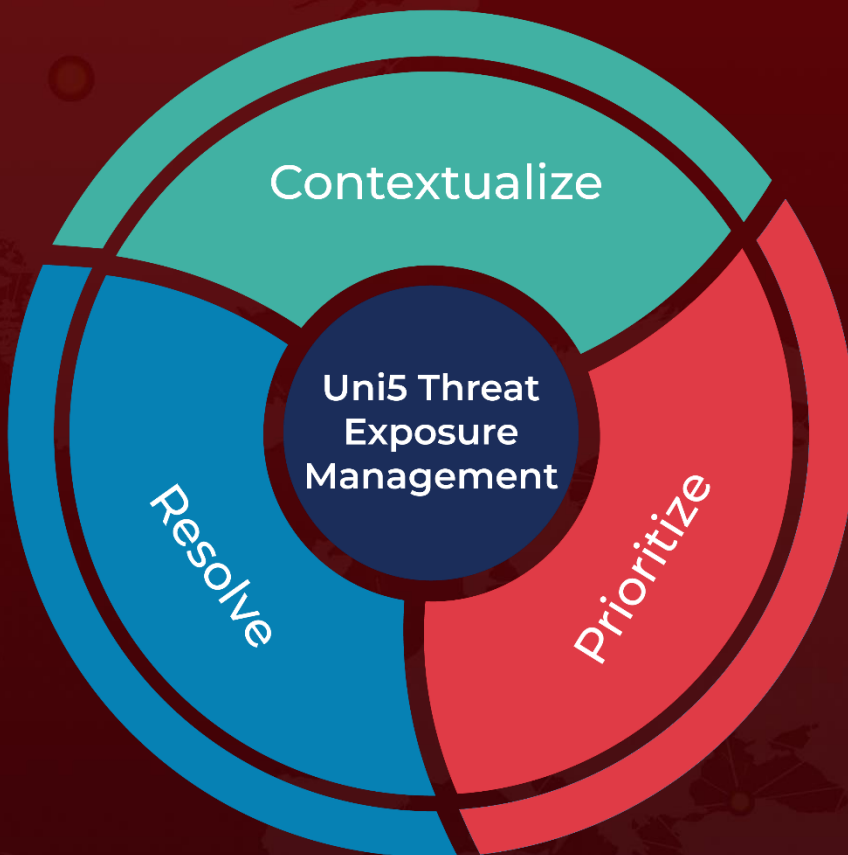
## References

<https://www.wordfence.com/blog/2024/03/critical-vulnerability-remains-unpatched-in-two-permanently-closed-miniorange-wordpress-plugins-1250-bounty-awarded/>

# What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

**March 19, 2024 • 7:30 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)