Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Vulnerability in WordPress Plugin threatens Website takeover

Date of Publication	Admiralty Code	TA Number
July 5, 2023	A1	TA2023286

Summary

First Seen: June 04, 2023
Affected Product: Ultimate Member WordPress Plugin
Severity: Critical, CVSS Score 9.8
Impact: WordPress Ultimate Member Plugin, with over 200K installations helps in streamlining user registration and login processes. It has been found vulnerable to unauthenticated privilege escalation, posing a potential risk of website takeover by attackers.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-3460	Unauthenticated Privilege Escalation Vulnerability	WordPress Ultimate Member Plugin	✓	✗	✓

Vulnerability Details

#1 WordPress Ultimate Member Plugin is used to create and manage website membership processes including new registration, login, content restriction and user profiles. This plugin is integrated with 200K websites.

#2 Multiple exploit activities related to WordPress websites were reported in June first week, later-on they were found to be related to Ultimate Member Plugin. The plugin does not prevent visitors from registering with arbitrary capabilities, thus allowing attackers to bestow administrator privileges.

#3 The Plugin employs negative security model of creating a block list of unallowed user metadata keys and does validation on each user registration. Attackers were able to bypass the restrictions with trivial methods.

#4 Attackers were found to be creating rogue user accounts with administrator privileges by modifying the "wp_capabilities" user meta value. Second stage of exploitation involved addition of malicious themes, malicious plugins and backdoors on the website.

#5 Plugin developers attempted to fix flaws with v2.6.4, v2.6.5 and v2.6.6, however they were found to be partial fix and final fix was provided with plugin v2.6.7.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-3460	WordPress Ultimate Member Plugin <= 2.6.6	cpe:2.3:a:ultimatemember:ultimate-member:2.6.5:*:*:*:*:wordpress:*:*	CWE-269

Recommendations

- **Update Plugin:** Update WordPress Ultimate Member Plugin to version 2.6.7 or above.
- **Validate Site data:** Verify site other resources including integrated plugins for any malicious content or backdoor.
- **Review Administrator Accounts:** Review all administrator accounts and delete any unknown account.
- **Reset Passwords:** Reset all administrators and user password. For user password, plugin developers shall be releasing new feature.
- **Send Advisories to your site members:** Inform site users on any suspicious breach so they can also verify and report any unknown activities with their account.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0003 Persistence	TA0004 Privilege Escalation	TA0043 Reconnaissance
T1595 Active Scanning	T1595.002 Vulnerability Scanning	T1068 Exploitation for Privilege Escalation	T1190 Exploit Public-Facing Application
T1136 Create Account	T1078 Valid Accounts		

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	exelica[.]com
IPv4	146.70.189[.]245, 103.187.5[.]128, 103.30.11[.]160, 103.30.11[.]146, 172.70.147[.]176

Patch Details

To address the vulnerability, it is essential to update to plugin version 2.6.7 or higher. Plugin version can be updated to required version via WordPress Admin dashboard.

References

https://blog.wpscan.com/hacking-campaign-actively-exploiting-ultimate-member-plugin/

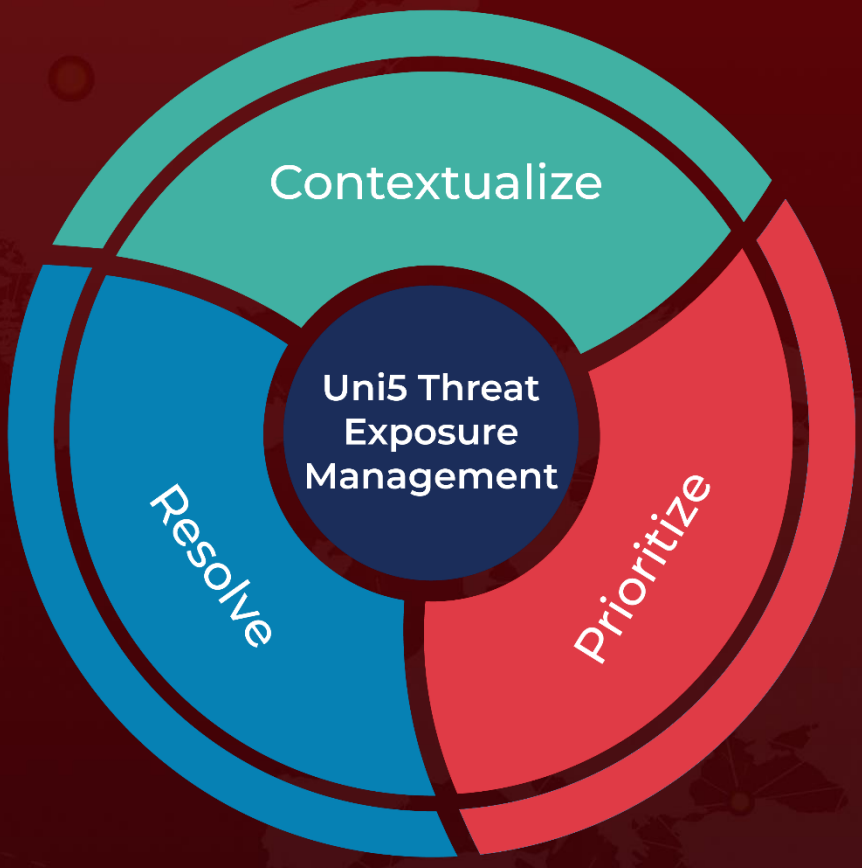
https://docs.ultimatemember.com/article/1866-security-incident-update-and-recommended-actions

https://github.com/ultimatemember/ultimatemember/releases/tag/2.6.7

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

July 05, 2023 • 08:30 AM

More at www.hivepro.com