Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Active Targeting of WP-Automatic Plugin Flaw Raises Concerns for Site Takeover

Date of Publication	Admiralty Code	TA Number
April 26, 2024	A1	TA2024166

Summary

Discovered On: March 13, 2024
Affected Products: WordPress Automatic plugin
Impact: The critical SQL Injection vulnerability (CVE-2024-27956) in the WP-Automatic plugin for WordPress poses a serious risk. Attackers could exploit this flaw to gain unauthorized access to websites, create admin accounts, upload malicious files, and potentially take complete control. Since the disclosure of the flaw, there have been over 5.5 million exploitation attempts detected.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-27956	WordPress Automatic Plugin SQL Injection Vulnerability	WordPress Automatic plugin	✗	✗	✓

Vulnerability Details

#1 A recent malware campaign has been targeting a critical flaw CVE-2024-27956 in the WordPress Automatic plugin, highlighting the ongoing threat posed by vulnerabilities in WordPress plugins. This vulnerability, known as an SQL injection (SQLi), is very serious because it could allow attackers to take complete control of affected websites. This particular vulnerability opens up various attack vectors, including bypassing authentication mechanisms, creating unauthorized admin accounts, uploading malicious files and renaming files for evasion.

#2 By leveraging the vulnerability in the WP-Automatic plugin, attackers gain the ability to execute unauthorized database queries, manipulate user accounts, and upload malicious files to the compromised server. Renaming the vulnerable plugin file is a tactic used by attackers to maintain exclusive access to the exploit and prevent others from exploiting it against the compromised website. This combination of actions allows attackers to take control of the website and carry out various malicious activities with potentially severe consequences.

#3 After obtaining admin access through the WP-Automatic plugin vulnerability, attackers may create backdoors to ensure continued access even if the initial exploit is patched or mitigated. These backdoors may be obfuscated to evade detection and removal, enabling attackers to maintain control of the compromised website and carry out further malicious activities without being easily detected by administrators or security measures.

#4 The vulnerability was publicly disclosed in mid-March 2024, and since then, there have been over 5.5 million attack attempts. This shows that attackers are actively trying to exploit this vulnerability, so it's important to take steps to protect your website.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-27956	WP-Automatic Plugin Version prior to 3.92.1	cpe:2.3:a:wordpress:automatic_plugin:*:*:*:*:*:*:*:*	CWE-89

Recommendations

- **Keep Plugins Updated:** Ensure that all WordPress plugins, including Automatic, are regularly updated to the latest versions to patch known vulnerabilities.
- **Implement a Web Application Firewall (WAF):** WAF play a crucial role in detecting and mitigating SQL injection attacks. They analyze HTTP requests in real-time, looking for suspicious patterns and signatures commonly associated with SQL injection attempts. By monitoring the behavior of web applications, WAF can identify abnormal activities indicative of an attack.
- **Regular Backup:** Establish a regular backup schedule to ensure that your website data is backed up consistently. Depending on the frequency of updates and changes to your website, daily or weekly backups may be appropriate.
- **Identify Unauthorized Users:** Check for any unauthorized or suspicious user accounts that may have been created without proper authorization. Look for accounts with administrative privileges that don't belong to legitimate users or accounts with unusual activity patterns. Disable or remove user accounts that are no longer needed or are inactive.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0004 Privilege Escalation	TA0005 Defense Evasion	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1059 Command and Scripting Interpreter	T1136 Create Account	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation
T1036 Masquerading	T1036.003 Rename System Utilities	T1584 Compromise Infrastructure	T1584.006 Web Services
T1027 Obfuscated Files or Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	b0ca85463fe805ffdf809206771719dc571eb052, 8e83c42ffd3c5a88b2b2853ff931164ebce1c0f3

Patch Details

Website administrators should promptly update the WP-Automatic plugin to version 3.92.1 to ensure that their sites are protected against this vulnerability.

Link: https://wpscan.com/vulnerability/53a51e79-a216-4ca3-ac2d-57098fd2ebb5/

References

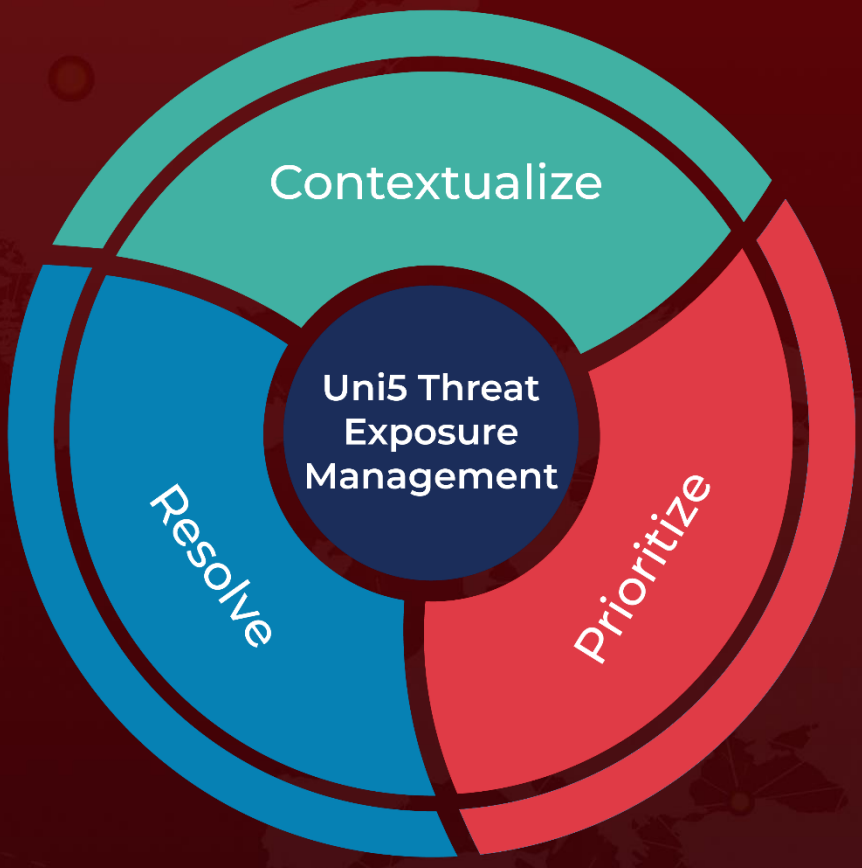
https://wpscan.com/blog/new-malware-campaign-targets-wp-automatic-plugin/

https://www.hivepro.com/threat-advisory/over-300k-wordpress-sites-affected-by-forminator-plugin-flaws/

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

April 26, 2024 • 7:00 AM

More at www.hivepro.com