Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Over 300k WordPress Sites Affected by Forminator Plugin Flaws

Date of Publication	Admiralty Code	TA Number
April 23, 2024	A1	TA2024159

Summary

Discovered On: April 2024
Affected Products: WordPress Forminator Plugin
Impact: The Forminator WordPress plugin, utilized by multiple websites, is vulnerable to multiple security flaws, including CVE-2024-28890, CVE-2024-31077, and CVE-2024-31857. These vulnerabilities enable malicious actors to carry out various attacks, including unrestricted file uploads to the server, triggering denial-of-service (DoS) attacks, and executing cross-site scripting (XSS) attacks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-28890	WordPress Forminator Plugin Unrestricted File Upload Vulnerability	WordPress Forminator Plugin	✗	✗	✓
CVE-2024-31077	WordPress Forminator Plugin SQL injection Vulnerability	WordPress Forminator Plugin	✗	✗	✓
CVE-2024-31857	WordPress Forminator Plugin Cross-site Scripting Vulnerability	WordPress Forminator Plugin	✗	✗	✓

Vulnerability Details

#1 Forminator Plugin, a widely-used form builder wordpress plugin with over 500,000 downloads, faces multiple security vulnerabilities, such as CVE-2024-28890, CVE-2024-31077, and CVE-2024-31857, impacting over 300,000 websites worldwide. Due to these vulnerabilities, threat actors may execute a variety of attacks, including as cross-site scripting (XSS) attacks, denial-of-service (DoS) assaults, and unlimited file uploads to the server.

#2 Forminator is a comprehensive form builder plugin designed to offer users the necessary functionality to create a wide range of forms, including contact forms, quizzes, and polls. With Forminator, users can easily design and customize forms to suit their specific needs.

#3 The CVE-2024-28890 vulnerability allows attackers to upload files to the server without any restrictions, potentially leading to the execution of arbitrary code or the compromise of sensitive data. CVE-2024-31077 permits threat actors to launch DoS attacks by exploiting certain functionalities of the plugin. Lastly, CVE-2024-31857 enables attackers to execute XSS attacks, potentially compromising user sessions and stealing sensitive information.

#4 Website administrators using the Forminator plugin should immediately update the plugin to address the vulnerabilities. Failure to do so could leave their websites vulnerable to exploitation by malicious actors, potentially leading to the unauthorized upload of malware. Although there are no public reports of active exploitation, the severity of the flaws and their ease of use highlight the importance of prompt action.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-28890	Forminator versions prior to 1.29.0	cpe:2.3:a:wpmu:forminator_plugin:*:*:*:*:*:*:*:*	CWE-434
CVE-2024-31077	Forminator versions prior to 1.29.3	cpe:2.3:a:wpmu:forminator_plugin:*:*:*:*:*:*:*:*	CWE-89
CVE-2024-31857	Forminator versions prior to 1.15.4	cpe:2.3:a:wpmu:forminator_plugin:*:*:*:*:*:*:*:*	CWE-79

Recommendations

Keep Plugins Updated: Ensure that all WordPress plugins, including Forminator, are regularly updated to the latest versions to patch known vulnerabilities.

Implement a Web Application Firewall (WAF): WAFs 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, WAFs can identify abnormal activities indicative of an attack.

Deploy Behavioral Analysis Solutions: Utilize behavioral analysis solutions to detect any anomalous behavior on systems. Ensure that endpoint protection solutions are regularly updated to identify and mitigate the latest threats.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0040 Impact	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1189 Drive-by Compromise	T1068 Exploitation for Privilege Escalation	T1498 Network Denial of Service	T1059 Command and Scripting Interpreter

Patch Details

Website administrators should promptly update the Forminator plugin to version 1.29.3 to ensure that their sites are protected against these vulnerabilities.

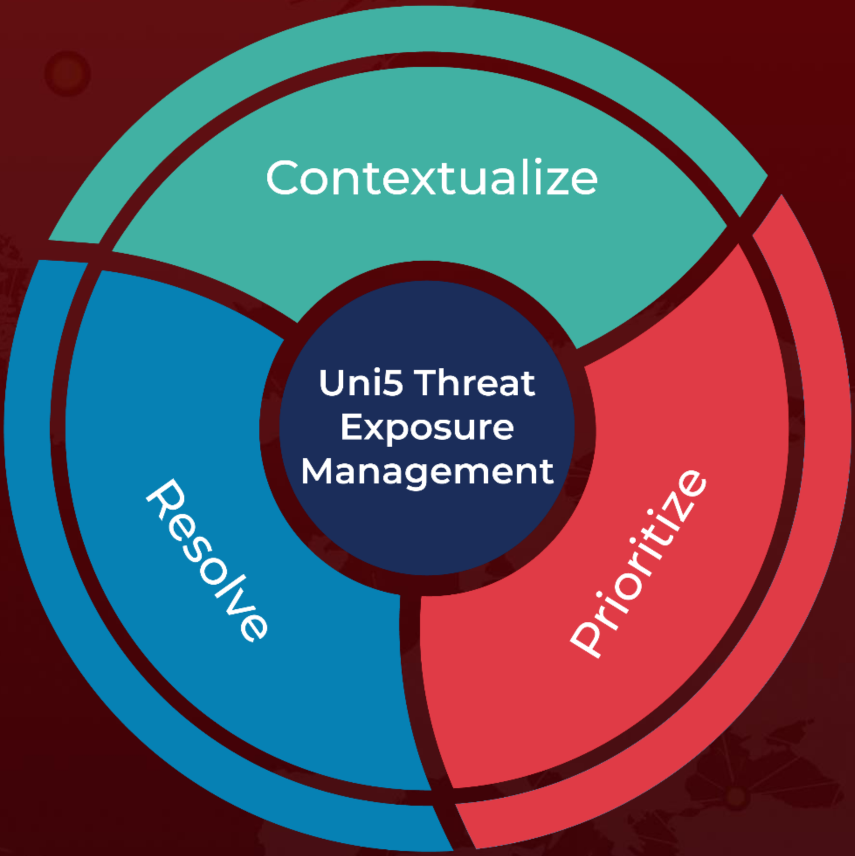
References

https://jvn.jp/en/jp/JVN50132400/

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 23, 2024 • 6:45 AM

More at www.hivepro.com