Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical RCE Flaw Found in Fortinet FortiClientLinux

Date of Publication	Admiralty Code	TA Number
April 11, 2024	A1	TA2024140

Summary

First Seen: April 9, 2024
Affected Platform: Fortinet FortiClientLinux
Impact: CVE-2023-45590 is a critical vulnerability in Fortinet FortiClientLinux that could allow attackers to remotely control your device if you visit a malicious website. This is critical because attackers can then run any program or steal information from your device. If you are using FortiClientLinux versions 7.2.0, 7.0.6 through 7.0.10, or 7.0.3 through 7.0.4, update to version 7.2.1 or 7.0.11 (or later) right away to protect yourself.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-45590	Fortinet FortiClient Remote Code Execution Vulnerability	Fortinet FortiClientLinux	☒	☒	✓

Vulnerability Details

#1 Fortinet has released patches to fix a critical vulnerability affecting FortiClientLinux, allowing arbitrary code execution. Identified as CVE-2023-45590 and boasting a CVSS score of 9.4, this vulnerability arises from improper code generation. It enables attackers to execute arbitrary code by deceiving users into accessing malicious websites.

#2 The affected versions include 7.0.3 through 7.0.4 and 7.0.6 through 7.0.10, mandating immediate upgrades to version 7.0.11 or higher. Additionally, version 7.2.0 requires upgrading to 7.2.1 or above to ensure protection. It is imperative for users to promptly update their systems to safeguard against potential threats posed by this critical vulnerability.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-45590	FortiClientLinux version 7.2.0, 7.0.6 through 7.0.10 and 7.0.3 through 7.0.4	cpe:2.3:a:fortinet:forticlient:*:*:*:*:*:*:*	CWE-94

Recommendations

Apply Patches: Immediately apply the patches provided by Fortinet for FortiClientLinux, FortiClientMac, FortiOS, and FortiProxy to address the identified vulnerabilities. Ensure that all affected versions are updated to the recommended versions or higher (7.0.11 or above for FortiClientLinux and 7.2.1 or above for FortiClientLinux version 7.2.0).

Network Segmentation: Implement network segmentation to limit the impact of potential attacks. Isolate critical systems and sensitive data from less secure areas of the network to prevent lateral movement by attackers.

Implement Web Filtering: Utilize web filtering solutions to block access to known malicious websites and prevent users from inadvertently visiting them. Regularly update the web filtering rules to adapt to evolving threats.

Vulnerability Scanning: Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0001 Initial Access	T1059 Command and Scripting Interpreter
T1588 Obtain Capabilities	T1203 Exploitation for Client Execution	T1588.005 Exploits	T1588.006 Vulnerabilities
T1189 Drive-by Compromise	T1036 Masquerading		

Patch Details

Upgrade FortiClientLinux 7.2 to version 7.2.1 or higher, and FortiClientLinux 7.0 to version 7.0.11 or above.

Link:
https://www.fortiguard.com/psirt/FG-IR-23-087

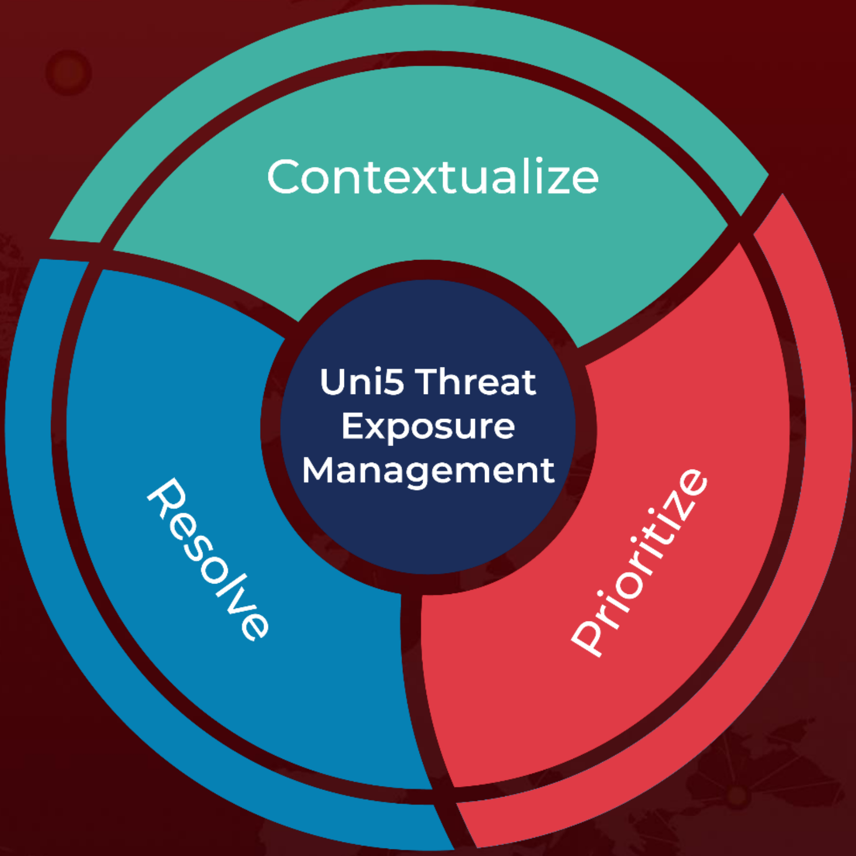
References

https://www.securityweek.com/fortinet-patches-critical-rce-vulnerability-in-forticlientlinux/

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 11, 2024 • 5:30 AM

More at www.hivepro.com