

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Fortinet Releases Patches for Critical Vulnerabilities in Various Products

Date of Publication

March 14, 2024

Last updated date

March 28, 2024

Admiralty Code

A1

TA Number

TA2024100










Summary

First Seen: March 12, 2024

Affected Platform: Fortinet FortiClientEMS, Fortinet FortiOS and Fortinet FortiProxy

Impact: A critical SQL Injection vulnerability (CVE-2023-48788) in FortiClientEMS software enables attackers to execute unauthorized code or commands via specially crafted HTTP requests. Additionally, two other critical bugs in FortiOS and FortiProxy have been addressed. Update promptly to patched versions to prevent potential exploitation.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-48788	Fortinet FortiClientEMS SQL Injection Vulnerability	Fortinet FortiClientEMS			
CVE-2023-42789	Fortinet FortiOS and FortiProxy Out-of-Bounds Write Vulnerability	Fortinet FortiOS and FortiProxy			
CVE-2023-42790	Fortinet FortiOS Stack-Based Buffer Overflow Vulnerability	Fortinet FortiOS and FortiProxy			

Vulnerability Details

#1

A critical vulnerability has been discovered in Fortinet FortiClientEMS software, labeled as CVE-2023-48788, which could allow attackers to execute unauthorized code or commands. The flaw, rated 9.3 out of 10 in severity, affects specific versions of FortiClientEMS, and users are advised to update to the patched versions promptly. This flaw is being exploited in wild and a POC exploit code is also publicly available.

#2

Additionally, Fortinet has addressed two other critical bugs in FortiOS and FortiProxy, identified as CVE-2023-42789 and CVE-2023-42790, which could also enable attackers to execute arbitrary code or commands. Recently Fortinet addressed a critical RCE vulnerability ([CVE-2024-21762](#)) in FortiOS SSL-VPN is actively exploited in the wild.

#3

The impacted product versions are listed, and users are urged to upgrade to the latest versions to mitigate these vulnerabilities. While there is no evidence of active exploitation yet, given past incidents of threat actors targeting unpatched Fortinet appliances, swift application of updates is strongly recommended.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-48788	FortiClientEMS 7.2.0 through 7.2.2 FortiClientEMS 7.0.1 through 7.0.10	cpe:2.3:a:fortinet:forticlient_enterprise_management_server:*:*:*:*:*:*:*	CWE-89
CVE-2023-42789	FortiOS version 7.4.0 through 7.4.1 FortiOS version 7.2.0 through 7.2.5 FortiOS version 7.0.0 through 7.0.12 FortiOS version 6.4.0 through 6.4.14 FortiOS version 6.2.0 through 6.2.15	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortiproxy:*:*:*:*:*:*:*	CWE-787
CVE-2023-42790	FortiProxy version 7.4.0 through 7.2.6 FortiProxy version 7.0.0 through 7.0.12 FortiProxy version 2.0.0 through 2.0.13		CWE-121

Recommendations



Apply Patches: Install the patches released by Fortinet promptly to fix the vulnerability. Patching is the most effective long-term solution.



Regular Software Updates: Establish a routine for monitoring and applying software updates from Fortinet. Regular updates help to address newly discovered vulnerabilities and strengthen the security posture of your systems.



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.



Network Segmentation: Implement network segmentation to limit the reach of potential attackers. This can help contain the impact of any successful exploitation.



Network Monitoring: Enhance network monitoring capabilities to detect any suspicious activity or unauthorized access attempts targeting the SSL VPN service.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0001</u> Initial Access	<u>T1190</u> Exploit Public-Facing Application
<u>T1588</u> Obtain Capabilities	<u>T1203</u> Exploitation for Client Execution	<u>T1588.005</u> Exploits	<u>T1588.006</u> Vulnerabilities
<u>T1059</u> Command and Scripting Interpreter			

Patch Details

Patched versions of Fortinet FortiClientEMS:

Upgrade to 7.2.3 or above

Upgrade to 7.0.11 or above

Patched versions of Fortinet FortiOS and FortiProxy:

FortiOS version 7.4.2 or above

FortiOS version 7.2.6 or above

FortiOS version 7.0.13 or above

FortiOS version 6.4.15 or above

FortiOS version 6.2.16 or above

FortiProxy version 7.4.1 or above

FortiProxy version 7.2.7 or above

FortiProxy version 7.0.13 or above

FortiProxy version 2.0.14 or above

Links:

<https://fortiguard.fortinet.com/psirt/FG-IR-24-007>

<https://fortiguard.fortinet.com/psirt/FG-IR-23-328>

References

<https://securityaffairs.com/160440/security/fortinet-critical-bugs-fortios-fortiproxy-forticlientems.html>

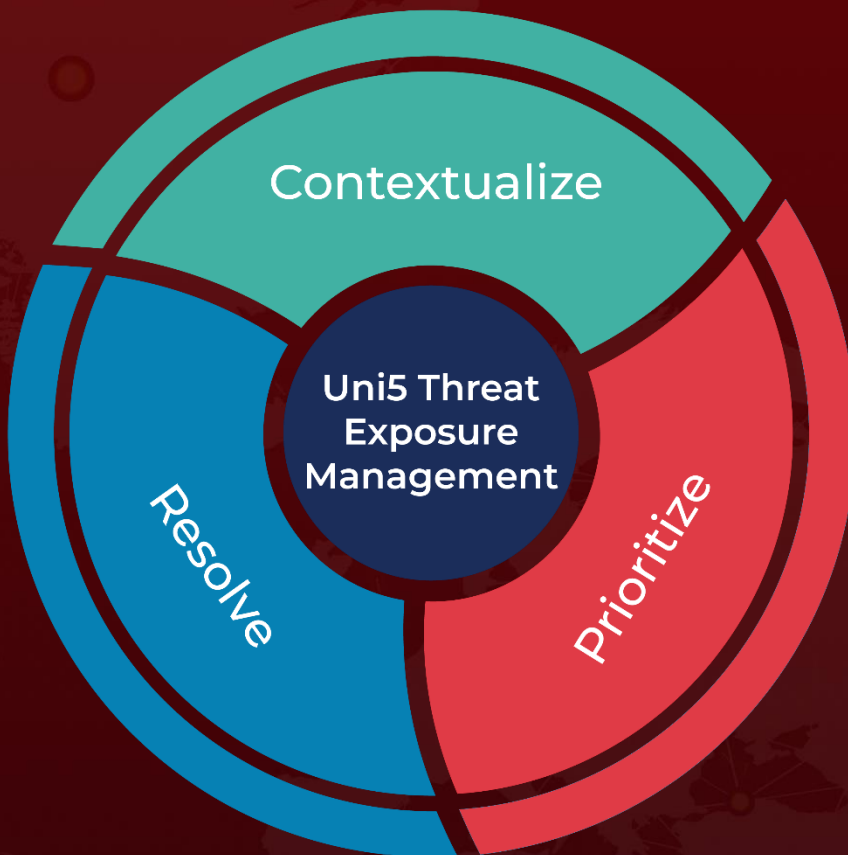
<https://www.hivepro.com/threat-advisory/critical-vulnerability-in-fortios-ssl-vpn-exploited-in-the-wild/>

<https://github.com/horizon3ai/CVE-2023-48788>

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 14, 2024 • 2:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com