

Hiveforce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Fortinet addresses Vulnerabilities in FortiADC, FortiOS and FortiProxy

Date of Publication

May 8, 2023

Admiralty Code

A1

TA Number

TA2023215







Summary

First Seen: May 3, 2023

Affected Product: FortiADC, FortiOS and FortiProxy

Impact: Arbitrary code execution via specifically crafted requests

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2023-27999	OS command vulnerability in FortiADC	FortiADC			
CVE-2023-22640	Out-of-Bounds write vulnerability in sslvpng	FortiOS and FortiProxy			

Vulnerability Details

Fortinet has released security updates for multiple products, including FortiADC, FortiOS, and FortiProxy, addressing nine vulnerabilities. Of these, two are classified as high-severity bugs. One vulnerability, tracked as CVE-2023-27999, is an improper neutralization of special elements used in an OS command vulnerability in FortiADC. An authenticated attacker could execute unauthorized commands through crafted arguments to existing commands. The other vulnerability, CVE-2023-22640, is an out-of-bounds write vulnerability in the sslvpng component of FortiOS and FortiProxy. An authenticated attacker can achieve arbitrary code execution by sending specially crafted requests.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-27999	FortiADC : 7.2.0, 7.1.1, 7.1.0	cpe:2.3:a:fortinet:fortiadc:*:*:*:*:*:*	CWE-78
CVE-2023-22640	FortiOS : 7.2.0 to 7.2.3, 7.0.0 to 7.0.10, 6.4.0 to 6.4.11, 6.2.0 to 6.2.13, 6.0.0 to 6.0.16; FortiProxy : 7.2.1, 7.2.0, 7.0.0 to 7.0.7, 2.0.0 to 2.0.12, 1.2.0 to 1.2.13, 1.1.0 to 1.1.6, 1.0.0 to 1.0.7	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:**, cpe:2.3:a:fortinet:fortiproxy:*:*:*:*:*:*	CWE-787

Recommendations



Disabling "Host Check", "Restrict to Specific OS Versions", and "MAC address host checking" in the sslvpn portal configuration can be a workaround solution to mitigate the CVE-2023-22640.



Apply the available security updates immediately: Fortinet has released patches for the vulnerabilities, so it is important to apply the available security updates as soon as possible to ensure that the systems are protected against potential attacks.



Implement least privilege access: Implementing the principle of least privilege access helps to limit the damage that an attacker can cause if they gain access to a system. Ensure that users are only given access to the resources and privileges that they need to perform their jobs.

Potential **MITRE ATT&CK** TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0040 Impact	T1133 External Remote Services	T1565 Data Manipulation
T1059 Command and Scripting Interpreter	T1574 Hijack Execution Flow	T1554 Compromise Client Software Binary	

Patch Details

<https://www.fortiguard.com/psirt/FG-IR-22-475>

<https://www.fortiguard.com/psirt/FG-IR-22-297>

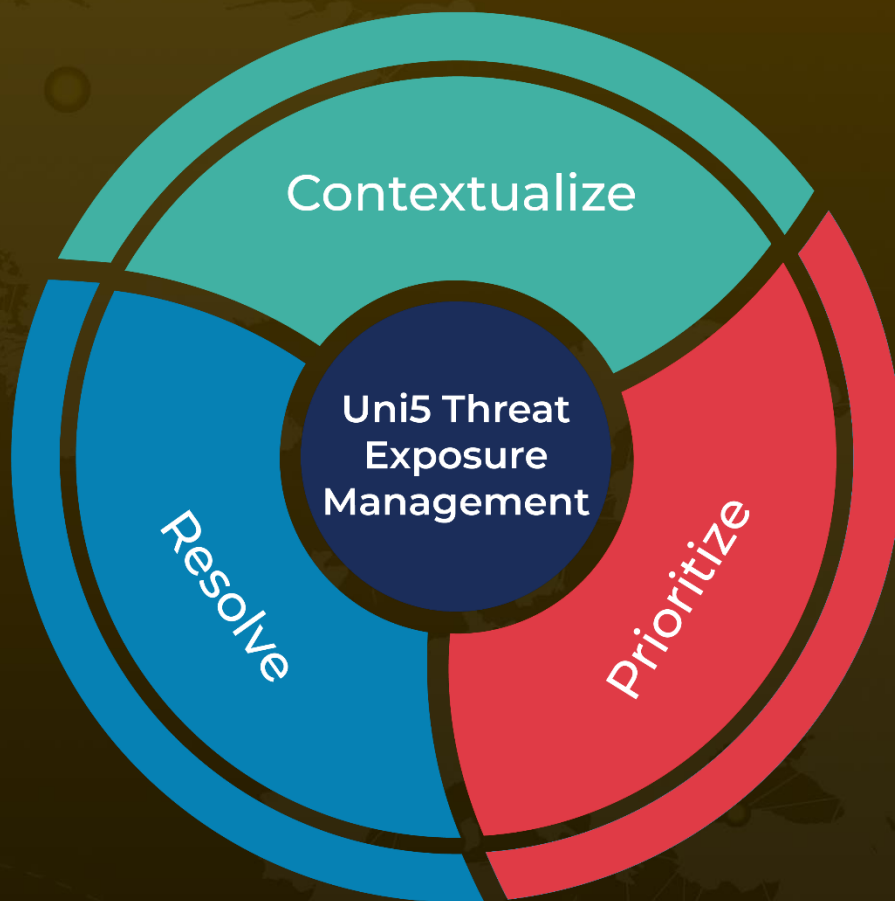
References

<https://www.securityweek.com/fortinet-patches-high-severity-vulnerabilities-in-fortiadc-fortios/>

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

May 8, 2023 • 1:30 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com