Hive Pro

Threat Level

Green

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Fortinet Addresses Security Flaws Across Multiple Products

Date of Publication	Admiralty code	TA Number
April 14, 2023	A1	TA2023187

Summary

First Seen: April 11, 2023
Affected Products: FortiAuthenticator, FortiProxy, FortiSIEM, FortiDDoS-F, FortiDDoS, FortiADC, FortiOS, FortiSOAR , FortiAnalyzer, FortiSandbox, FortiDeceptor, FortiWeb, FortiManager, and FortiClient for Windows and macOS
Impact: Arbitrary code execution allows an attacker to gain access to sensitive information.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-40679	Fortinet Command injection Vulnerability	FortiDDoS-F, FortiDDoS, & FortiADC	✗	✗	✓
CVE-2022-40682	FortiClient Incorrect Authorization Vulnerability	FortiClient Windows	✗	✗	✓
CVE-2022-43946	FortiClient Improper write access Vulnerability	FortiClient Windows	✗	✗	✓
CVE-2022-42470	FortiClientWindows Path Traversal Vulnerability	FortiClient Windows	✗	✗	✓
CVE-2022-41330	Fortinet Cross-Site Scripting Vulnerability	FortiProxy & FortiOS	✗	✗	✓
CVE-2022-41331	FortiPresence Critical Function Vulnerability	FortiPresence	✗	✗	✓
CVE-2023-27995	FortiSOAR Server-side Template Injection	FortiSOAR	✗	✗	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2022-27487	Fortinet Improper Privilege Management Vulnerability	FortiDeceptor & FortiSandbox	✗	✗	✓
CVE-2022-43955	FortiWeb Cross-Site Scripting Vulnerability	FortiWeb	✗	✗	✓

Vulnerability Details

Fortinet has addressed vulnerabilities discovered in several products, including FortiOS, FortiProxy, FortiSandbox, FortiDeceptor, FortiWeb, FortiClient for Windows and macOS, FortiSOAR, FortiADC, FortiDDoS, FortiDDoS-F, FortiAnalyzer, and FortiManager. These vulnerabilities had the potential to cause various security issues, such as cross-site scripting (XSS) attacks, unauthorized API calls, command execution, arbitrary code and file execution, privilege escalation, and information disclosure. Fortinet has also addressed multiple vulnerabilities of medium and low severity affecting FortiNAC, FortiOS, FortiProxy, FortiADC, FortiGate, and FortiAuthenticator.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-40679	FortiADC: 7.1.0-5.0.0 & FortiDDoS: 4.0.0 - 6.4.0	cpe:2.3:a:fortinet:fortiadc:-:*:*:*:*:*:*:* cpe:2.3:a:fortinet:FortiDDoS:-:*:*:*:*:*:*:*	CWE-78
CVE-2022-40682	Fortinet FortiClient for Windows: 7.0.7-6.0.0	cpe:2.3:a:fortinet:fortinet_forticlient:-:*:*:*:*:*:*:*	CWE-863
CVE-2022-43946	Fortinet FortiClient for Windows: 7.0.7- 6.0.0	cpe:2.3:a:fortinet:fortinet_forticlient:-:*:*:*:*:*:*:*	CWE-732 CWE-367

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-42470	Fortinet FortiClient for Windows: 7.0.7-6.0.0	cpe:2.3:a:fortinet:fortinet_forticlient:-:*:*:*:*:*:*:*	CWE-23
CVE-2022-41330	FortiOS: 7.2.3-6.2.0 & FortiProxy: 7.0.0 - 7.2.1	cpe:2.3:o:fortinet:fortios:-:*:*:*:*:*:*:* cpe:2.3:o:fortinet:fortiproxy:-:*:*:*:*:*:*:*	CWE-79
CVE-2022-41331	FortiPresence: 1.0.0 - 1.2.1	cpe:2.3:a:fortinet:fortipresence:-:*:*:*:*:*:*:*	CWE-306
CVE-2023-27995	FortiSOAR: 7.3.0 - 7.3.1	cpe:2.3:a:fortinet:fortisoar:-:*:*:*:*:*:*:*	CWE-1336
CVE-2022-27487	FortiSandbox: 2.5.0 - 4.2.2 & FortiDeceptor: 1.0.0 - 4.1.0	cpe:2.3:a:fortinet:fortisandbox:-:*:*:*:*:*:*:*	CWE-269
CVE-2022-43955	Fortinet FortiWeb: 6.3.0 - 7.0.3	cpe:2.3:a:fortinet:fortinet_fortiweb:-:*:*:*:*:*:*:*	CWE-79

Recommendations

We highly recommend updating your installations as soon as possible to address the vulnerabilities mentioned above. Although these vulnerabilities are not currently being exploited in attacks, unpatched Fortinet products have been targeted in the past by malicious actors, including nation-state threat actors. Taking prompt action to apply the necessary updates can significantly reduce the risk of compromise and help protect against potential attacks.

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Patch Links

https://www.fortiguard.com/psirt/FG-IR-22-335

https://www.fortiguard.com/psirt/FG-IR-22-336

https://www.fortiguard.com/psirt/FG-IR-22-429

https://www.fortiguard.com/psirt/FG-IR-22-320

https://www.fortiguard.com/psirt/FG-IR-22-363

https://www.fortiguard.com/psirt/FG-IR-22-355

https://www.fortiguard.com/psirt/FG-IR-23-051

https://www.fortiguard.com/psirt/FG-IR-22-056

https://www.fortiguard.com/psirt/FG-IR-22-428

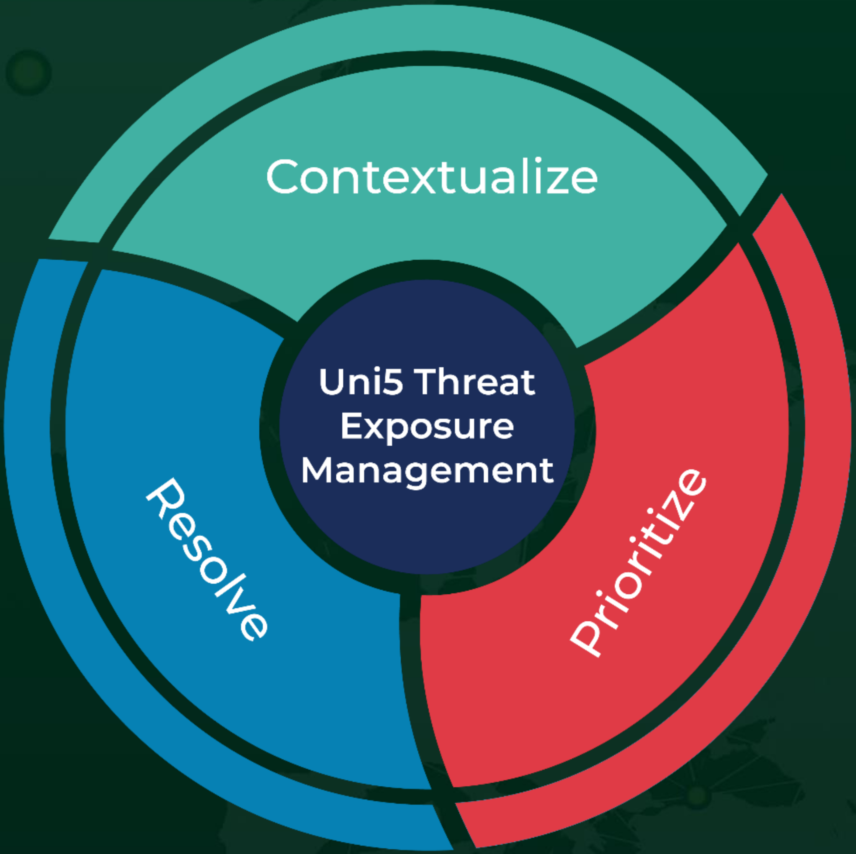
References

https://www.fortiguard.com/psirt?date=04-2023

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 14, 2023 • 6:45 AM

More at www.hivepro.com