Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Multiple Vulnerabilities in Various Fortinet Products in March 2023

Date of Publication	Admiralty Code	TA Number
March 10, 2023	A1	TA2023129

Summary

First Seen: March 7, 2023
Affected Product: FortiManager, FortiAnalyzer, FortiPortal, FortiNAC, FortiWeb, FortiRecorder, FortiWeb, FortiSOAR, FortiAuthenticator, FortiDeceptor, FortiMail, FortiOS, FortiProxy & FortiSwitch
Impact: Attackers could gain access to unauthorized or sensitive information about the network, cause a denial of service (DoS), inject malicious code into a webpage.

CVEs

CVE	NAME	PATCH
CVE-2022-41329	FortiOS / FortiProxy - Unauthenticated access to static files containing logging information	✓
CVE-2022-42476	FortiOS / FortiProxy - Path traversal vulnerability allows VDOM escaping	✓
CVE-2023-25610	FortiOS / FortiProxy - Heap buffer underflow in administrative interface	✓
CVE-2022-41328	FortiOS - Path traversal in execute command	✓
CVE-2022-45861	FortiOS & FortiProxy - Access of NULL pointer in SSLVPNd	✓
CVE-2023-23776	FortiAnalyzer - log-fetch client request password is shown in clear text in the heartbeat response	✓

CVE	NAME	PATCH
CVE-2022-40676	FortiNAC - Multiple Reflected XSS	✓
CVE-2022-39953	FortiNAC - Multiple privilege escalation via sudo command	✓
CVE-2022-27490	FortiManager, FortiAnalyzer, FortiPortal & FortiSwitch - Information disclosure through diagnose debug commands	✓
CVE-2023-25611	FortiAnalyzer - CSV injection in macro name	✓
CVE-2022-29056	FortiAuthenticator, FortiDeceptor & FortiMail - Improper restriction over excessive authentication attempts	✓
CVE-2023-25605	FortiSOAR - Improper Authorization in request headers	✓
CVE-2022-39951	FortiWeb - command injection in webserver	✓
CVE-2022-41333	FortiRecorder - DoS in login authentication mechanism	✓
CVE-2022-22297	FortiWeb and FortiRecorder - Arbitrary file read through command line pipe	✓

Vulnerability Details

In March 2023, Fortinet issued several vulnerabilities that impact various products, including FortiOS, FortiProxy, FortiAnalyzer, FortiNAC, FortiManager, FortiPortal, FortiSwitch, FortiAuthenticator, FortiDeceptor, FortiMail, FortiSOAR, FortiWeb, and FortiRecorder. These vulnerabilities range from unauthenticated access to sensitive information to denial-of-service attacks and privilege escalation. One warns of a NULL pointer access vulnerability in SSLVPNd in both FortiOS and FortiProxy, while another describes a path traversal vulnerability that enables VDOM escaping. A third reports an improper restriction on excessive authentication attempts, leading to a partial denial of service. A fourth warns of an information disclosure vulnerability that allows unauthorized access to static files containing logging information in FortiOS and FortiProxy. Finally, the fifth highlights a heap buffer underflow vulnerability in the administrative interface of FortiOS and FortiProxy, which impacts multiple versions of these products.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-41329	FortiProxy: 7.0.0 - 7.2.2 FortiOS: 6.2.3 - 6.2.13, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3, 6.4.0 - 6.4.11	cpe:2.3:h:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*, cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	CWE-200
CVE-2022-42476	FortiOS: 6.4.0 - 6.4.11, 7.2.0 - 7.2.3, 6.2.0 - 6.2.12, 7.0.0 - 7.0.7	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	CWE-23
CVE-2022-22297	Fortinet FortiWeb: 6.1.0 - 6.1.3, 6.0.0 - 6.0.8, 6.3.0 - 6.3.17, 6.2.0 - 6.2.7, 6.4.0 - 6.4.1, FortiRecorder: 2.7.0 - 6.4.3	cpe:2.3:a:fortinet:fortinet_fortiweb:*:*:*:*:*:*:*:*:*, cpe:2.3:h:fortinet:fortirecorder:*:*:*:*:*:*:*:*:*	CWE-792
CVE-2023-25611	FortiAnalyzer: 7.0.0 - 7.0.5, 6.4.0 - 6.4.9, 7.2.0 - 7.2.1	cpe:2.3:a:fortinet:fortianalyzer:*:*:*:*:*:*:*:*:*	CWE 1236

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-25610	FortiOS: 6.0.0 - 6.0.16, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3, 6.2.0 - 6.2.12, 6.4.0 - 6.4.11, FortiProxy: 1.1.0 - 7.2.2	cpe:2.3:h:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*, cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	CWE-124
CVE-2022-41328	FortiOS: 6.4.0 - 6.4.11, 6.2.0 - 6.2.13, 6.0.0 - 6.0.16, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3	cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	CWE-22
CVE-2022-45861	FortiOS: 6.2.0 - 6.2.13, 7.0.0 - 7.0.9, 7.2.0 - 7.2.3, 6.4.0 - 6.4.11, FortiProxy: 1.1.5 - 7.2.1	cpe:2.3:h:fortinet:fortiproxy:*:*:*:*:*:*:*:*:*, cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*:*:*:*	CWE-824
CVE-2022-29056	FortiAuthenticator : 6.4.0 - 6.4.6, 6.3.0 - 6.3.4, 6.2.0 - 6.2.2, 6.1.0 - 6.1.3, 6.0.0 - 6.0.8, 5.5.0, 5.4.0 - 5.4.1, 5.3.0 - 5.3.1, 5.2.0 - 5.2.2, 5.1.0 - 5.1.2 FortiMail : 6.4.0, 6.2.1 - 6.2.4, 6.0.0 - 6.0.9, 5.4.0 - 5.4.11 FortiDeceptor : 3.1.1, 3.0.0 - 3.0.2, 2.1.0, 2.0.0, 1.1.0, 1.0.1, 1.0.0	cpe:2.3:a:fortinet:fortiauthenticator:-:*:*:*:*:*:*:*:*, cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:*:*, cpe:2.3:a:fortinet:fortideceptor:*:*:*:*:*:*:*:*:*	CWE-307
CVE-2023-25605	FortiSOAR: 7.3.0 - 7.3.1	cpe:2.3:a:fortinet:fortisoar:*:*:*:*:*:*:*:*:*	CWE-284
CVE-2022-39951	Fortinet FortiWeb: 7.0.0 - 7.0.2, 6.3.7 - 6.3.20, 6.4.0 - 6.4.2	cpe:2.3:a:fortinet:fortinet_fortiweb:*:*:*:*:*:*:*:*:*	CWE-78
CVE-2022-41333	FortiRecorder: 6.0.0 - 6.4.3	cpe:2.3:h:fortinet:fortirecorder:*:*:*:*:*:*:*:*:*	CWE-400
CVE-2022-39953	FortiNAC: 8.3.7 - 9.4.1	cpe:2.3:a:fortinet:fortinac:*:*:*:*:*:*:*:*:*	CWE-269
CVE-2022-40676	FortiNAC: 8.3.7 - 9.4.0	cpe:2.3:a:fortinet:fortinac:*:*:*:*:*:*:*:*:*	CWE-79

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-23776	FortiAuthenticator : 6.4.0 - 6.4.6, 6.3.0 - 6.3.4, 6.2.0 - 6.2.2, 6.1.0 - 6.1.3, 6.0.0 - 6.0.8, 5.5.0, 5.4.0 - 5.4.1, 5.3.0 - 5.3.1, 5.2.0 - 5.2.2, 5.1.0 - 5.1.2 FortiMail : 6.4.0, 6.2.1 - 6.2.4, 6.0.0 - 6.0.9, 5.4.0 - 5.4.11 FortiDeceptor : 3.1.1, 3.0.0 - 3.0.2, 2.1.0, 2.0.0, 1.1.0, 1.0.1, 1.0.0	cpe:2.3:a:fortinet:fortiauthenticator:-:*:*:*:*:*:*:*, cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:*, cpe:2.3:a:fortinet:fortideceptor:*:*:*:*:*:*:*:*	CWE-200
CVE-2022-27490	FortiManager : 6.0.0 - 6.0.4, 5.6.0 - 5.6.11 FortiAnalyzer : 6.0.0 - 6.0.4, 5.6.1, 5.6.0 - 5.6.11 FortiPortal : 6.0.0 - 6.0.9, 5.3.0 - 5.3.8, 5.2.0 - 5.2.6, 5.1.0 - 5.1.2, 5.0.0 - 5.0.3, 4.2.0 - 4.2.2, 4.1.0 - 4.1.2 FortiSwitch : 7.0.0 - 7.0.4, 6.4.0 - 6.4.10, 6.2.0 - 6.2.7, 6.0.0 - 6.0.7	cpe:2.3:a:fortinet:fortimanager:-:*:*:*:*:*:*:*, cpe:2.3:a:fortinet:fortianalyzer:*:*:*:*:*:*:*:*, cpe:2.3:a:fortinet:fortiportal:-:*:*:*:*:*:*:*, cpe:2.3:h:fortinet:fortiswitch:*:*:*:*:*:*:*:*	CWE-200

Recommendations

Security Leaders

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.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0008 Lateral Movement	**T1543** Create or Modify System Process	**T1190** Exploit Public-Facing Application	**T1210** Exploitation of Remote Services
T1078 Valid Accounts	**T1098** Data from Local System	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities

Patch Details

https://www.fortiguard.com/psirt/FG-IR-22-477

https://www.fortiguard.com/psirt/FG-IR-22-401

https://www.fortiguard.com/psirt/FG-IR-20-078

https://www.fortiguard.com/psirt/FG-IR-22-364

https://www.fortiguard.com/psirt/FG-IR-23-001

https://www.fortiguard.com/psirt/FG-IR-23-050

https://www.fortiguard.com/psirt/FG-IR-22-488

https://www.fortiguard.com/psirt/FG-IR-22-254

https://www.fortiguard.com/psirt/FG-IR-22-388

https://www.fortiguard.com/psirt/FG-IR-22-447

https://www.fortiguard.com/psirt/FG-IR-21-218

https://www.fortiguard.com/psirt/FG-IR-22-369

https://www.fortiguard.com/psirt/FG-IR-22-281

https://www.fortiguard.com/psirt/FG-IR-22-309

https://www.fortiguard.com/psirt/FG-IR-18-232

https://www.fortiguard.com/psirt/FG-IR-21-218

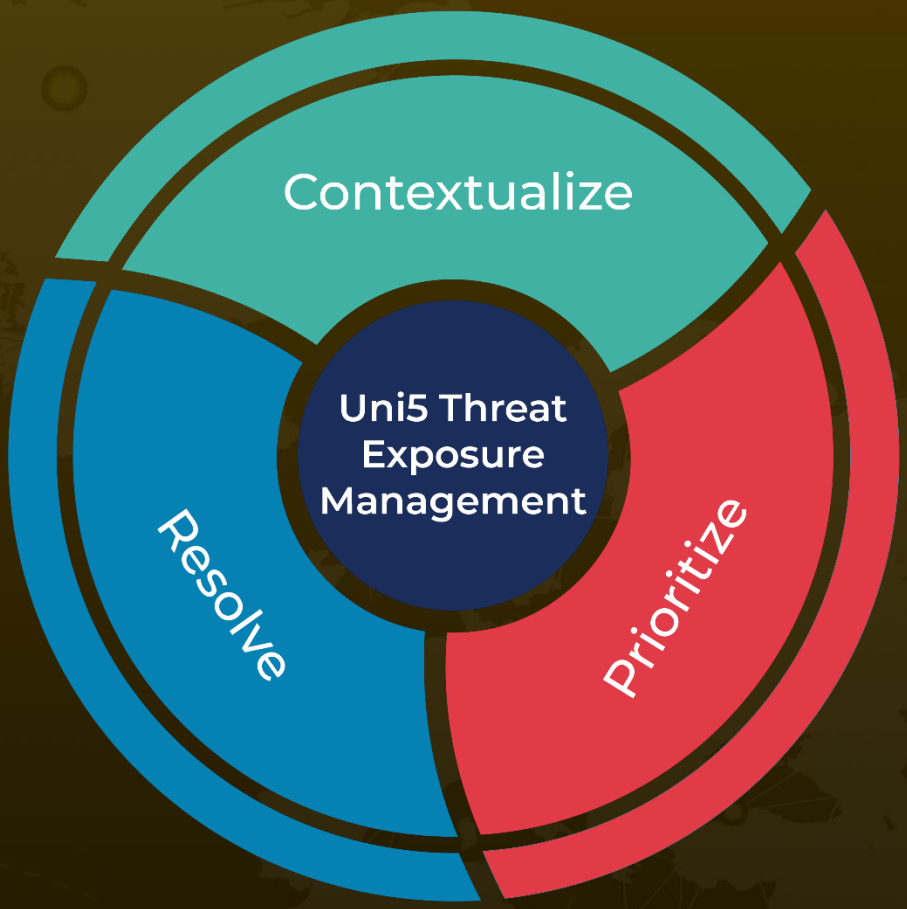
References

https://www.fortiguard.com/psirt-monthly-advisory/march-2023-vulnerability-advisories

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 10, 2023 • 4:15 PM

More at www.hivepro.com