

THREAT ADVISORY

VULNERABILITY REPORT

Fortinet addresses Authentication Bypass in addition to numerous flaws

Date of Publication

December 8, 2022

Admiralty Code

A1

TA Number

TA2022290







Summary

First Seen: December 6, 2022

Affected Products: FortiOS, FortiADC, FortiProxy, FortiSandbox, FortiSOAR, and FortiDeceptor

Impact: Insufficient access control and execution of unauthorized code

CVEs

CVE	NAME	PATCH
CVE-2022-35843	RADIUS authentication bypass in SSH component	
CVE-2022-33876	Improper input validation in download	
CVE-2022-33875	SQL injection vulnerability in configuration backup	
CVE-2022-40680	Stored cross-site scripting in replacement messages visualization	
CVE-2022-38379	HTML Injection in FortiSOAR	
CVE-2022-30305	Insufficient logging of failed authentication attempts	

Vulnerability Details

Fortinet addressed security flaws across its products, including a high-severity authentication bypass affecting FortiOS and FortiProxy tracking CVE-2022-35843 in FortiOS's SSH login component. Only when Radius authentication is utilized can the bug be triggered. A remote attacker can circumvent authentication and get access to the device by delivering a specially designed Access-Challenge response from the Radius server. Other weaknesses allow an authenticated attacker to retrieve files and execute arbitrary code via crafted HTTP requests.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-35843	FortiOS : 7.2.1 - 6.4.9 and FortiProxy : 2.0.0 - 7.0.6	cpe:2.3:o:fortinet:fortios:-:*:*:*:*:* cpe:2.3:h:fortinet:fortiproxy:-:*:*:*:*:*	CWE-302
CVE-2022-33876	FortiADC : 7.0.0 - 5.1.0	cpe:2.3:a:fortinet:fortiadc:-:*:*:*:*:*	CWE-20
CVE-2022-33875	FortiADC : 7.0.2 - 5.2.8	cpe:2.3:a:fortinet:fortiadc:7.0.0:*:*:*:*:*	CWE-89
CVE-2022-40680	FortiOS : 7.2.0 - 7.2.1, 7.0.0 - 7.0.6	cpe:2.3:o:fortinet:fortios:7.2.1:*:*:*:*:*	CWE-79
CVE-2022-38379	FortiSOAR: 7.0.0 - 7.0.3, 7.2.0	cpe:2.3:a:fortinet:fortisoar:7.0.0:*:*:*:*:*	CWE-79
CVE-2022-30305	FortiDeceptor: 3.0.0 - 4.2.0 and FortiSandbox: 3.1.0 - 4.0.2	cpe:2.3:a:fortinet:fortideceptor:-:*:*:*:*:* cpe:2.3:a:fortinet:fortisandbox:-:*:*:*:*:*	CWE-778

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

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0003</u> Persistence
<u>TA0008</u> Lateral Movement	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1078</u> Valid Accounts
<u>T1098</u> Account Manipulation	<u>T1203</u> Exploitation for Client Execution	<u>T1190</u> Exploit Public-Facing Application	<u>T1574</u> Hijack Execution Flow
<u>T1210</u> Exploitation of Remote Services	<u>T1059</u> Command and Scripting Interpreter		

Patch Links

<https://www.fortiguard.com/psirt/FG-IR-22-253>

<https://www.fortiguard.com/psirt/FG-IR-22-252>

<https://www.fortiguard.com/psirt/FG-IR-22-255>

<https://www.fortiguard.com/psirt/FG-IR-21-248>

<https://www.fortiguard.com/psirt/FG-IR-22-220>

<https://www.fortiguard.com/psirt/FG-IR-21-170>

References

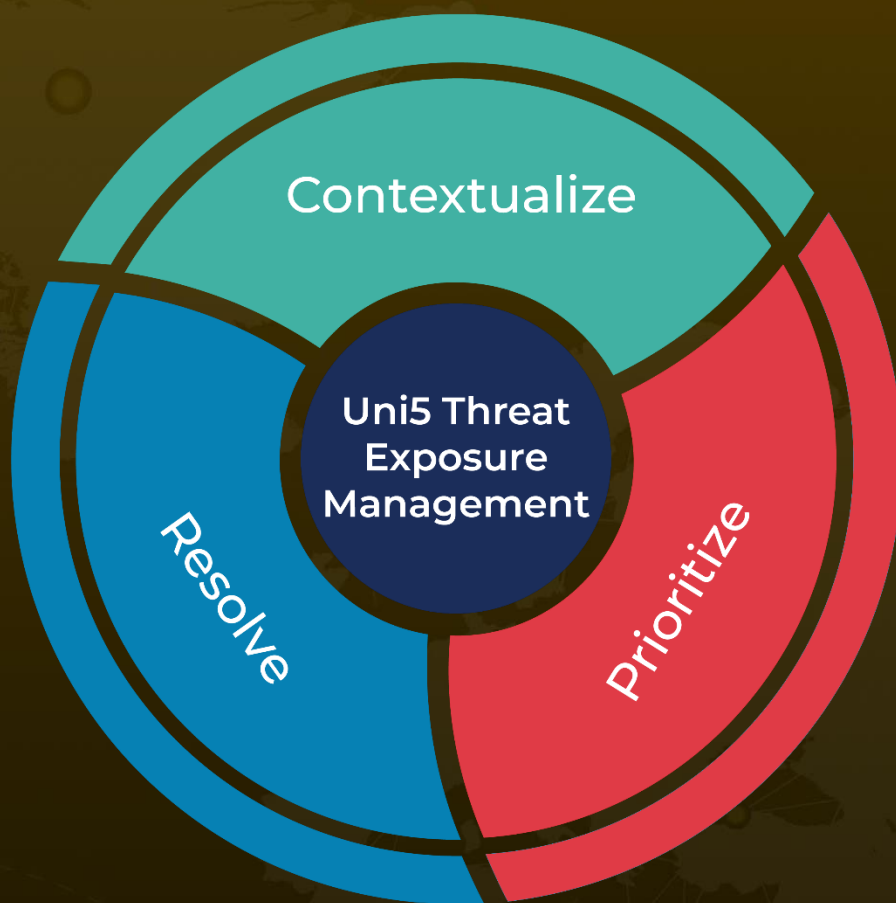
<https://www.fortiguard.com/psirt?date=12-2022>

<https://www.securityweek.com/fortinet-patches-high-severity-authentication-bypass-vulnerability-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

December 8, 2022 • 5:45 AM

© 2022 All Rights are Reserved by HivePro



More at www.hivepro.com