

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Multiple Fortinet products are vulnerable to unauthorized code execution flaws

Date of Publication

February 20, 2023

Admiralty Code

A1

TA Number

TA2023090







Summary

First Seen: February 16, 2023

Affected Products: FortiWeb, FortiOS, FortiNAC, and FortiProxy

Impact: Exploiting these vulnerabilities could enable local attackers to escalate privileges and execute unauthorized code or commands, potentially leading to significant security breaches.

CVE

CVE	NAME	PATCH
CVE-2022-39952	External Control of File Name or Path in keyUpload scriptlet	
CVE-2021-42756	Stack-based buffer overflows in Proxyd	
CVE-2022-27482	OS command injection vulnerability in CLI	
CVE-2022-27489	Multiple command injection vulnerabilities in webserver	
CVE-2022-38375	Unauthenticated access to administrative operations in FortiNAC	
CVE-2023-23780	Multiple Stack based buffer overflow in web interface	

Vulnerability Details

#1

Fortinet has released security patches to address vulnerabilities in its product range, including two critical vulnerabilities that impact FortiNAC and FortiWeb solutions. One of the vulnerabilities, identified as CVE-2022-39952, affects the FortiNAC network access control solution and is related to external control of the file name or path in the FortiNAC web server. This vulnerability could allow unauthenticated attackers to execute arbitrary writes on the system.

#2

The second noteworthy flaw is CVE-2021-42756, which involves multiple stack-based buffer overflow vulnerabilities in the proxy daemon of FortiWeb, the web application firewall solution. The vulnerability can be triggered by an unauthenticated remote attacker using a specially crafted HTTP request, which may lead to arbitrary code execution.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-39952	FortiNAC versions: 8.3.7 - 9.4.0	cpe:2.3:a:fortinet:fortinac:-:*:*:*:*:*	CWE-73
CVE-2021-42756	FortiWeb versions: 6.4 – 5.6.0	cpe:2.3:a:fortinet:fortiweb:-:*:*:*:*:*	CWE-121
CVE-2022-27482	FortiADC versions: 7.0.1 - 5.0.4	cpe:2.3:a:fortinet:fortiadc:-:*:*:*:*:*	CWE-78
CVE-2022-27489	FortiExtender versions: 7.0.3 - 3.0.0	cpe:2.3:h:fortinet:fortiextender:-:*:*:*:*:*	CWE-78
CVE-2022-38375	FortiNAC versions: 9.4.1 - 9.2.0	cpe:2.3:a:fortinet:fortinac:-:*:*:*:*:*	CWE-285
CVE-2023-23780	Fortinet FortiWeb versions: 7.0.1 - 6.3.20	cpe:2.3:a:fortinet:fortinet_fortiweb:-:*:*:*:*:*	CWE-121

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	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1543 Create or Modify System Process
T1210 Exploitation of Remote Services	T1190 Exploit Public-Facing Application	T1078 Valid Accounts	T1098 Account Manipulation

Patch Links

<https://www.fortiguard.com/psirt/FG-IR-22-300>
<https://www.fortiguard.com/psirt/FG-IR-21-186>
<https://www.fortiguard.com/psirt/FG-IR-22-046>
<https://www.fortiguard.com/psirt/FG-IR-22-048>
<https://www.fortiguard.com/psirt/FG-IR-22-329>
<https://www.fortiguard.com/psirt/FG-IR-22-118>

References

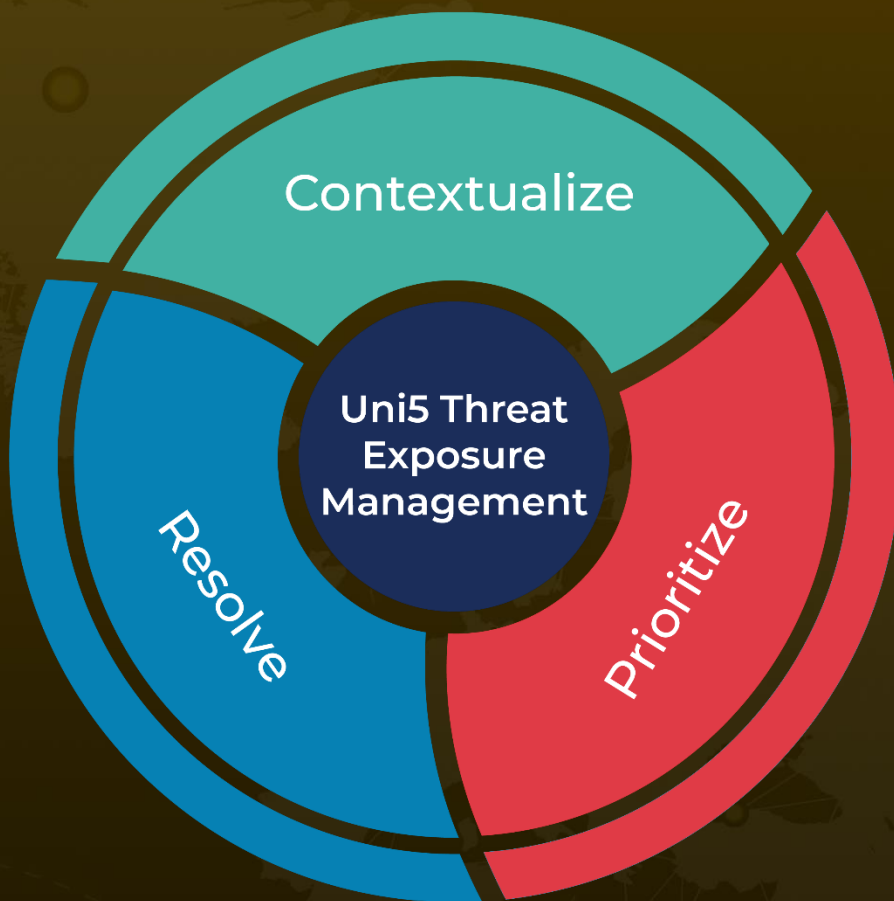
<https://www.fortiguard.com/psirt?page=2&date=02-2023>

<https://thehackernews.com/2023/02/fortinet-issues-patches-for-40-flaws.html>

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

February 20, 2023 • 3:10 AM

© 2023 All Rights are Reserved by HivePro



More at www.hivepro.com