Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Fortinet Addressed Critical RCE FortiNAC Vulnerability

Date of Publication	Admiralty Code	TA Number
June 27, 2023	A1	TA2023280

Summary

First Seen: June 19, 2023
Affected Product: FortiNAC
Impact: The vulnerabilities allow attackers to gain unauthorized access, and remote code execution, compromising network security and potentially exposing sensitive data.

CVEs

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2023-33299	FortiNAC Remote Code Execution Vulnerability	FortiNAC	✗	✗	✓
CVE-2023-33300	FortiNAC Command Injection Vulnerability	FortiNAC	✗	✗	✓

Vulnerability Details

#1

Fortinet has released patches for a critical vulnerability in its FortiNAC network access control solution. The vulnerability tracked as CVE-2023-33299 with a CVSS score of 9.6, involves the deserialization of untrusted data that can lead to remote code execution. An attacker could exploit this vulnerability to execute unauthorized code or commands through specially crafted requests to the TCP/1050 service. The affected versions of FortiNAC include 7.2.1, 9.4.2, 9.2.7, 9.1.9, and all 8.x iterations. Fortinet has addressed the issue with the release of FortiNAC versions 7.2.2, 9.4.3, 9.2.8, and 9.1.10, excluding the 8.x versions.

#2

Additionally, Fortinet resolved another vulnerability, CVE-2023-33300, which involves a medium-severity command injection via FortiNAC's TCP/5555 service. This vulnerability allows an unauthenticated attacker to copy local files to other directories on the device through specially crafted input fields. However, access to the copied data requires an existing foothold and sufficient privileges on the device. The issue was fixed with the release of FortiNAC versions 7.2.2 and 9.4.4.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-33299	FortiNAC : 9.4.2, 9.4.1, 9.4.0, 9.2.7, 9.2.6, 9.2.5, 9.2.4, 9.2.3, 9.2.2, 9.2.1, 9.2.0, 9.1.9, 9.1.8, 9.1.7, 9.1.6, 9.1.5, 9.1.4, 9.1.3, 9.1.2, 9.1.1, 9.1.0, 8.8.9, 8.8.8, 8.8.7, 8.8.6, 8.8.5, 8.8.4, 8.8.3, 8.8.2, 8.8.11, 8.8.10, 8.8.1, 8.8.0, 8.7.6, 8.7.5, 8.7.4, 8.7.3, 8.7.2, 8.7.1, 8.7.0, 8.6.5, 8.6.4, 8.6.3, 8.6.2, 8.6.1, 8.6.0, 8.5.4, 8.5.3, 8.5.2, 8.5.1, 8.5.0, 8.3.7, 7.2.1, 7.2.0	cpe:2.3:a:fortinet:fortinac:9.4.2:*:*:*:*:*:*:*	CWE-502
CVE-2023-33300	FortiNAC : 9.4.3, 9.4.2, 9.4.1, 9.4.0, 7.2.1, 7.2.0	cpe:2.3:a:fortinet:fortinac:9.4.2:*:*:*:*:*:*:*	CWE-77

Recommendations

Apply the latest patches: Ensure that you promptly apply the security updates provided by Fortinet for FortiNAC. Upgrade to the recommended versions (FortiNAC 9.4.4 or above, FortiNAC 9.2.8 or above, FortiNAC 9.1.10 or above, and FortiNAC 7.2.2 or above) to address the identified vulnerabilities. Keeping the software up to date with the latest patches is crucial to prevent potential exploitation.

Limit exposure to the public internet: As mentioned, one of the vulnerabilities (CVE-2023-33299) requires access to the TCP/1050 service. To reduce the risk of exploitation, restrict external access to this service by implementing proper network segmentation and firewall rules. Minimizing exposure of critical services to the public internet helps mitigate potential attacks.

Enforce strong access controls: Implement strict access controls and authentication mechanisms for FortiNAC deployments. Utilize strong passwords, two-factor authentication, and role-based access control (RBAC) to ensure that only authorized personnel can access and make changes to the FortiNAC system.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0010 Exfiltration	TA0007 Discovery	TA0009 Collection
TA0005 Defense Evasion	T1190 Exploit Public-Facing Application	T1082 System Information Discovery	T1005 Data from Local System
T1016 System Network Configuration Discovery	T1059 Command and Scripting Interpreter	T1083 File and Directory Discovery	

Patch Link

https://www.fortiguard.com/psirt/FG-IR-23-074

https://www.fortiguard.com/psirt/FG-IR-23-096

References

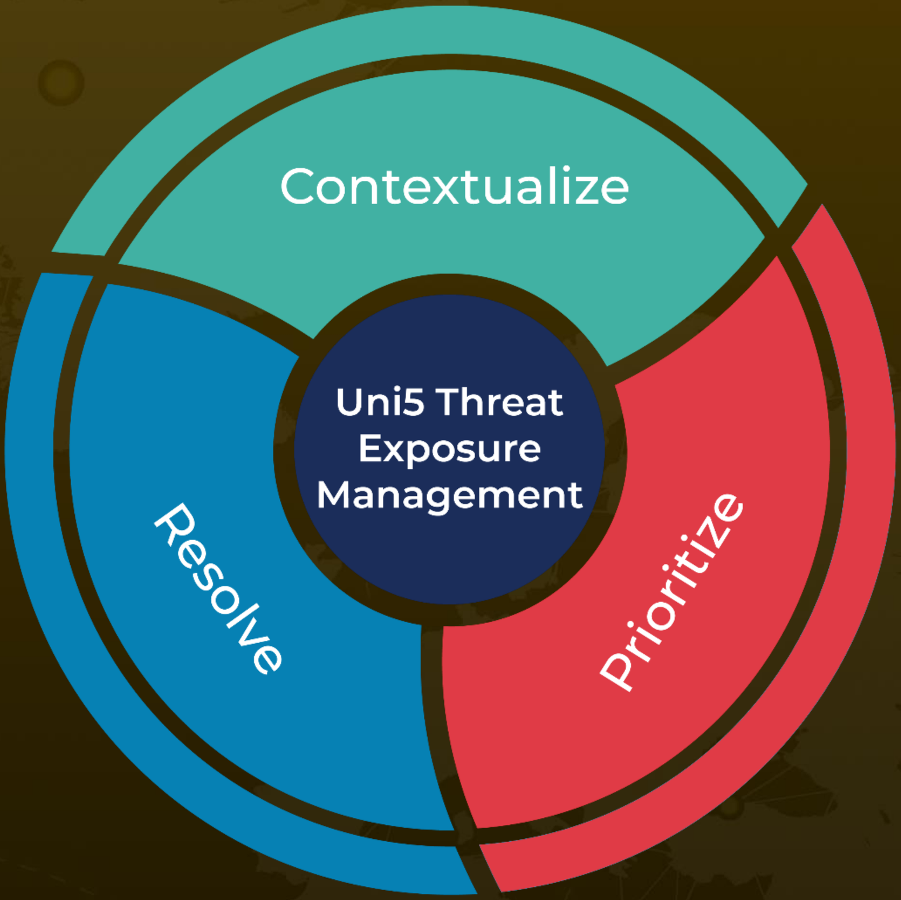
https://www.securityweek.com/fortinet-patches-critical-rce-vulnerability-in-fortinac/

https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-fortinac-remote-command-execution-flaw/

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

June 27, 2023 • 03:30 AM

More at www.hivepro.com