

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Fortinet Firewalls Under Siege: Exploitation of Critical Zero-Day CVE-2024-55591

Date of Publication

January 20, 2025

Admiralty Code

A1

TA Number

TA2025011




Summary

First Seen: November 16, 2024

Affected Products: Fortinet FortiOS and FortiProxy

Impact: A recently identified zero-day vulnerability in FortiOS and FortiProxy, tracked as CVE-2024-55591, is being actively exploited by threat actors to compromise Fortinet firewalls and breach enterprise networks. This critical flaw enables remote attackers to bypass authentication mechanisms and escalate their access to super-admin privileges. By leveraging specially crafted requests targeting the Node.js websocket module, attackers can exploit the vulnerability to gain full control over affected systems, posing a severe risk to organizational security.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-55591	Fortinet FortiOS Authorization Bypass Vulnerability	Fortinet FortiOS and FortiProxy			

Vulnerability Details

#1

Attackers are actively exploiting CVE-2024-55591, a critical zero-day vulnerability in FortiOS and FortiProxy, to compromise Fortinet firewalls and infiltrate enterprise networks. This vulnerability, stemming from an authentication bypass in the Node.js websocket module, allows threat actors to craft malicious requests and gain super-admin privileges, leading to severe breaches and unauthorized device control.

#2

In December 2024, researchers uncovered a targeted campaign leveraging this flaw against FortiGate firewall devices with internet-exposed management interfaces. The attack unfolded in four stages: vulnerability scanning from November 16–23, reconnaissance from November 22–27, configuration changes to SSL VPN settings between December 4–7, and lateral movement within compromised networks from December 16–27.

#3

During the campaign, attackers made significant modifications to firewall management interfaces, creating new local user accounts per device, granting these accounts super-admin privileges, and adding them to existing SSL VPN groups. They also created new SSL VPN portals and established tunnels with compromised devices. The operation culminated in the use of DCSync to extract credentials for lateral movement. However, the attackers purged traces of their activities before advancing further, leaving their ultimate objectives unknown.

#4

A notable aspect of the campaign was the frequent, automated use of the jsonconsole interface from a small number of suspicious IP addresses, with login events occurring within seconds. This pattern of activity highlights the attackers' efficiency and precision in targeting vulnerable devices. This incident serves as a stark reminder of the critical need to secure management interfaces against public exposure. Organizations must restrict access to management interfaces to trusted internal networks and users.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-55591	FortiOS Versions 7.0.0 through 7.0.16, FortiProxy Versions 7.2.0 through 7.2.12, FortiProxy Versions 7.0.0 through 7.0.19	cpe:2.3:a:fortinet:fortiproxy:*.:*:*:*:*:* cpe:2.3:o:fortinet:fortios:*:*:*:*:*:*	CWE-288

Recommendations



Apply Patch: Upgrade FortiOS and FortiProxy to the latest patched versions provided by Fortinet to address CVE-2024-55591. Regularly check for firmware updates.



Restrict Management Interface Access: Disable public exposure of management interfaces. Restrict access to trusted internal networks or implement a VPN for secure administrative access.



Limit Administrative Privileges: Adopt a least-privilege access model, granting super-admin rights only to essential accounts. Regularly review and audit user permissions.



Implement Multi-Factor Authentication (MFA): Enable MFA for all administrative accounts and VPN user accounts to reduce the risk of unauthorized access.



Administrative Interface Security: To mitigate potential security risks, you can either disable the HTTP/HTTPS administrative interface or restrict its access to specific IP addresses. By implementing either of these options, you can effectively secure the administrative interface from unauthorized access, reducing the risk of exploitation.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0042 Resource Development	TA0001 Initial Access	TA0003 Persistence
TA0008 Lateral Movement	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application
T1136 Create Account	T1136.001 Local Account	T1133 External Remote Services	T1078 Valid Accounts
T1078.001 Default Accounts	T1003 OS Credential Dumping	T1003.006 DCSync	

🔪 Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	23[.]27[.]140[.]65, 66[.]135[.]27[.]178, 157[.]245[.]3[.]251, 45[.]55[.]158[.]47, 167[.]71[.]245[.]10, 137[.]184[.]65[.]71, 155[.]133[.]4[.]175, 31[.]192[.]107[.]165, 37[.]19[.]196[.]65, 64[.]190[.]113[.]25

🔪 Patch Details

Promptly update to latest version of FortiOS and FortiProxy, as these versions includes the necessary patch to address the vulnerability.

FortiOS 7.0 Upgrade to 7.0.17 or above

FortiProxy 7.2 Upgrade to 7.2.13 or above

FortiProxy 7.0 Upgrade to 7.0.20 or above

Link: <https://fortiguard.fortinet.com/psirt/FG-IR-24-535>

🔪 References

<https://fortiguard.fortinet.com/psirt/FG-IR-24-535>

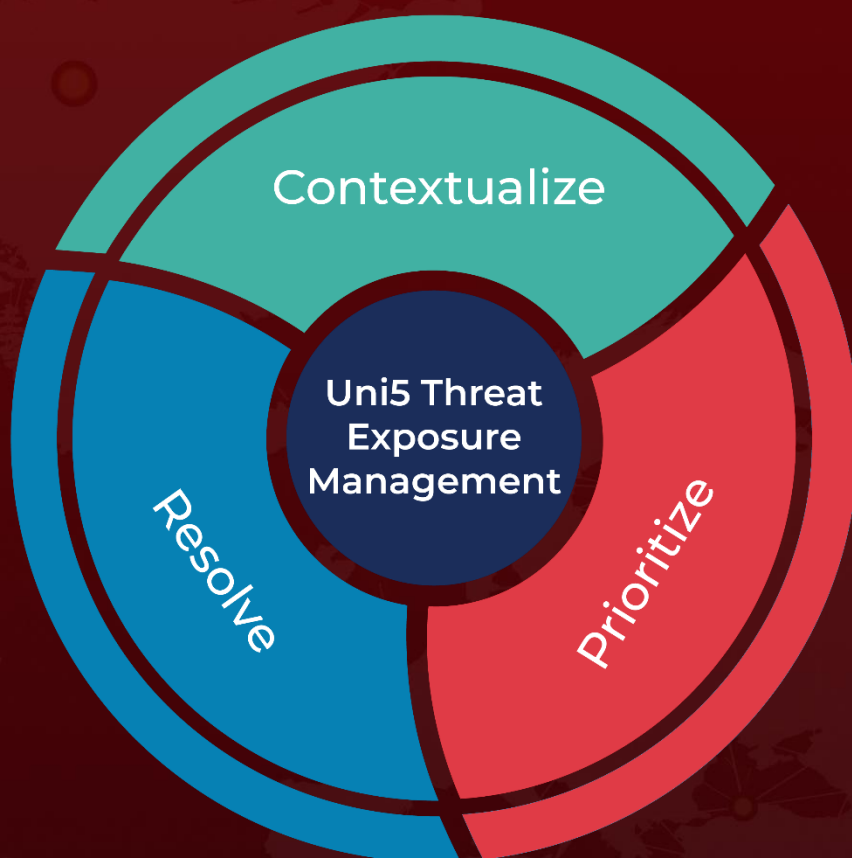
<https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/>

<https://github.com/watchtowrlabs/fortios-auth-bypass-check-CVE-2024-55591>

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

January 20, 2025 • 5:10 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com