Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Exploited in the Wild: Fortinet Urges Patch for Critical Zero-Day

Date of Publication	Admiralty Code	TA Number
May 14, 2025	A1	TA2025148

Summary

First Seen: May 2025
Affected Products: Fortinet FortiVoice, FortiMail, FortiNDR, FortiRecorder and FortiCamera
Impact: A critical zero-day vulnerability (CVE-2025-32756), a stack-based buffer overflow in Fortinet products, is being actively exploited in the wild. Threat actors are leveraging this flaw to execute malicious commands remotely, perform network reconnaissance, and steal credentials. Fortinet has released patches, and users are strongly urged to update immediately or disable web admin access to mitigate the risk.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-32756	Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability	Fortinet FortiVoice, FortiMail, FortiNDR, FortiRecorder and FortiCamera	✓	✓	✓

Vulnerability Details

#1

Fortinet has addressed a critical security flaw, tracked as CVE-2025-32756, which has already been exploited in the wild. This critical vulnerability affects multiple Fortinet products, including FortiVoice, FortiMail, FortiNDR, FortiRecorder, and FortiCamera.

#2 The issue stems from a stack-based buffer overflow vulnerability that could let an attacker run unauthorized commands or code by sending specially crafted HTTP requests. What's especially concerning is that attackers do not need to log in to exploit this flaw, they can do it remotely and without authentication.

#3 The vulnerability has been actively exploited in the wild, particularly against FortiVoice devices. In these attacks, threat actors scanned networks, deleted system crash logs to cover their tracks, and turned on debugging features to capture user credentials from system or SSH login attempts.

#4 If you use any of the affected products, it’s crucial to apply the security patches immediately. If patching right away isn’t feasible, a strong temporary workaround is to disable the HTTP/HTTPS administrative interface to block potential exploitation. Prompt action is key to preventing further compromise.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-32756	FortiCamera Version 2.1.0 through 2.1.3 FortiCamera 2.0 All Versions FortiCamera 1.1 All Versions FortiMail Version 7.6.0 through 7.6.2 FortiMail Version 7.4.0 through 7.4.4 FortiMail Version 7.2.0 through 7.2.7 FortiMail Version 7.0.0 through 7.0.8 FortiNDR Version 7.6.0 FortiNDR Version 7.4.0 through 7.4.7 FortiNDR Version 7.2.0 through 7.2.4 FortiNDR 7.1 All Versions FortiNDR Version 7.0.0 through 7.0.6 FortiNDR 1.1 – 1.5 All Versions FortiRecorder Version 7.2.0 through 7.2.3 FortiRecorder Version 7.0.0 through 7.0.5 FortiRecorder Version 6.4.0 through 6.4.5 FortiVoice Version 7.2.0 FortiVoice Version 7.0.0 through 7.0.6 FortiVoice Version 6.4.0 through 6.4.10	cpe:2.3:a:fortinet:fortivoice:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortirecorder:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortindr:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:fortimail:*:*:*:*:*:*:*:* cpe:2.3:a:fortinet:forticamera:*:*:*:*:*:*:*:*	CWE-121

Recommendations

Update Immediately: Make sure to install the latest security updates from Fortinet for products like FortiVoice, FortiMail, FortiNDR, FortiRecorder, and FortiCamera. These patches fix a critical flaw that attackers are actively exploiting, so updating now is the best way to protect your systems.

Turn Off Web Admin Access If You Can't Update Yet: If you're not able to install the patch right away, temporarily disable the HTTP/HTTPS admin interface. This will help block the attack route and reduce the risk of hackers getting in until you can apply the necessary updates.

Audit Devices and Lock Down Admin Access: Review all Fortinet devices in your network to ensure they're up to date and not exposed, especially older or less frequently maintained ones. At the same time, restrict access to admin panels by applying firewall rules or using a VPN, so only trusted IP addresses can reach them. This helps reduce risk and strengthens your overall security posture.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0010** Exfiltration	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities
T1059 Command and Scripting Interpreter	**T1566** Phishing	**T1053** Scheduled Task/Job	**T1053.003** Cron
T1068 Exploitation for Privilege Escalation			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4410352e110f82eabc0bf160bec41d21, ebce43017d2cb316ea45e08374de7315, 489821c38f429a21e1ea821f8460e590, 364929c45703a84347064e2d5de45bcd, 2c8834a52faee8d87cff7cd09c4fb946
IPv4	198[.]105[.]127[.]124, 43[.]228[.]217[.]173, 43[.]228[.]217[.]82, 156[.]236[.]76[.]90, 218[.]187[.]69[.]244, 218[.]187[.]69[.]59
SHA256	6e123e7f3202a8c1e9b1f94d8941580a25135382b99e8d3e34fb858bba311348, 27e409705b29937b9a6105038d9c2e3eb8dc3e2c8d606d22872dbde7f47c000f

Patch Details

Update your Fortinet products to the latest version to address the flaw.

Links:
https://fortiguard.fortinet.com/psirt/FG-IR-25-254

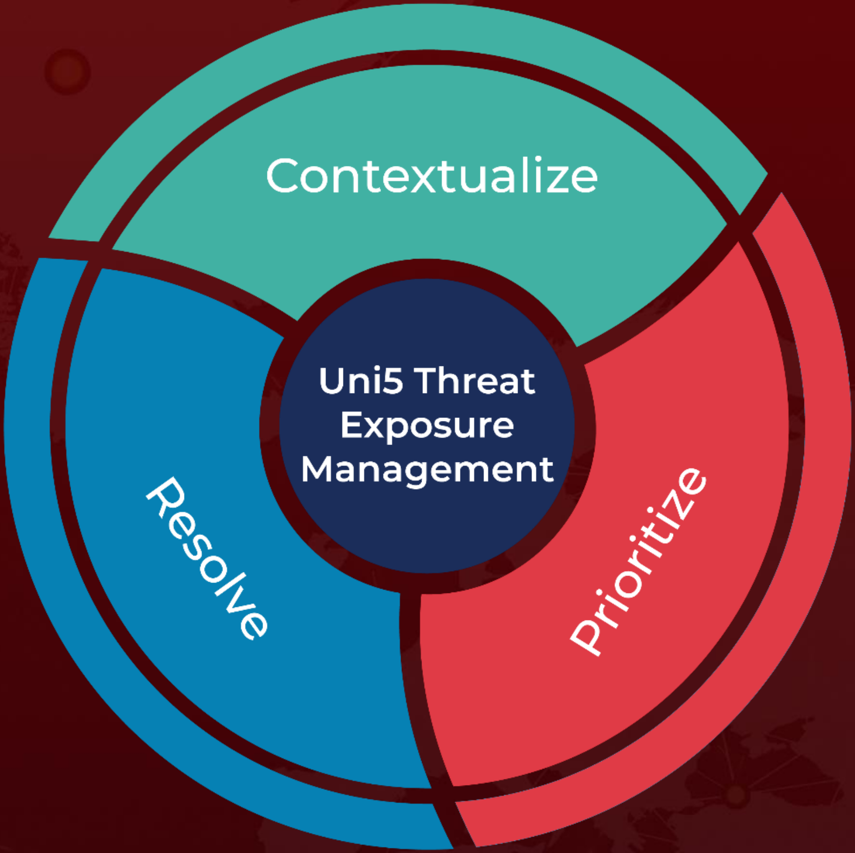
References

https://fortiguard.fortinet.com/psirt/FG-IR-25-254

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

May 14, 2025 • 4:30 AM

More at www.hivepro.com