

CVE-2025-32756

Fortinet Multiple Products Stack-Based Buffer Overflow Vulnerability

CISA KEV since May 14, 2025

Actively exploited

A stack-based buffer overflow vulnerability [CWE-121] vulnerability in Fortinet FortiCamera 2.1.0 through 2.1.3, FortiCamera 2.0 all versions, FortiCamera 1.1 all versions, FortiMail 7.6.0 through 7.6.2, FortiMail 7.4.0 through 7.4.4, FortiMail 7.2.0 through 7.2.7, FortiMail 7.0.0 through 7.0.8, FortiNDR 7.6.0, FortiNDR 7.4.0 through 7.4.7, FortiNDR 7.2.0 through 7.2.4, FortiNDR 7.0.0 through 7.0.6, FortiRecorder 7.2.0 through 7.2.3, FortiRecorder 7.0.0 through 7.0.5, FortiRecorder 6.4.0 through 6.4.5, FortiVoice

EVRS 75_{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.309 98.3rd percentile · FIRST	CISA DEADLINE Jun 4, 2025 KEV since 2025 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.309 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

7.2.0, FortiVoice 7.0.0 through 7.0.6, FortiVoice 6.4.0 through 6.4.10 allows a remote unauthenticated attacker to execute arbitrary code or commands via sending HTTP requests with specially crafted hash cookie.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortimail	$\geq 7.0.0 < 7.0.9$ $\geq 7.2.0 < 7.2.8$ $\geq 7.4.0 < 7.4.5$ $\geq 7.6.0 < 7.6.3$	7.0.9 · 7.2.8 · 7.4.5 · 7.6.3	NVD
fortindr	$\geq 7.0.0 < 7.0.7$ $\geq 7.2.0 < 7.2.5$ $\geq 7.4.0 < 7.4.8$ 1.1.0 1.2.0 1.3.0 1.4.0 1.5.0 7.1.0 7.1.1 7.6.0	7.0.7 · 7.2.5	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
fortirecorder	$\geq 6.4.0 < 6.4.6$ $\geq 7.0.0 < 7.0.6$ $\geq 7.2.0 < 7.2.4$	no fixed version listed	NVD
fortivoice	$\geq 6.4.0 < 6.4.11$ $\geq 7.0.0 < 7.0.7$ 7.2.0	no fixed version listed	NVD
forticamera firmware	$\geq 2.0.0 \leq 2.1.3$ $\geq 1.1.0 \leq 1.1.5$	no fixed version listed	NVD
forticamera	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-fcpx-h44g-vx2x
NVD nvd.nist.gov/vuln/detail/CVE-2025-32756

Additional guidance fortiguard.fortinet.com/psirt/FG-IR-25-254
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2025-14705

Current data evulnable.com/vulnerability-management/cve/CVE-2025-32756

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.