

Forum:[Hack Forums](#)

Thread: [Fortinet Releases Security Advisory for Relative Path Traversal Vulnerability Affect](#)

Stanley - November 30, 2025, 6:20 am

Fortinet Releases Security Advisory for Relative Path Traversal Vulnerability Affect

CISA has updated this Alert to include an additional vulnerability, CVE-2025-58034, and its relation to CVE-2025-64446, and associated resources.

CISA is aware of the exploitation of two vulnerabilities, CVE-2025-64446 and CVE-2025-58034, in Fortinet FortiWeb, a web application firewall. CISA is also aware that threat actors could exploit CVE-2025-64446 as an initial access vector and then chain CVE-2025-58034 to escalate privileges on a target system. These vulnerabilities chained together could lead to unauthenticated remote code execution against vulnerable FortiWeb products.

CVE-2025-64446 affects the following FortiWeb versions:1

- 8.0.0 through 8.0.1
- 7.6.0 through 7.6.4
- 7.4.0 through 7.4.9
- 7.2.0 through 7.2.11
- 7.0.0 through 7.0.11

CVE-2025-58034 affects the following FortiWeb versions:2

- 8.0.0 through 8.0.1
- 7.6.0 through 7.6.5
- 7.4.0 through 7.4.10
- 7.2.0 through 7.2.11
- 7.0.0 through 7.0.11

CVE-2025-64446 is a relative path traversal vulnerability (CWE-23: Relative Path Traversal) that may allow an unauthenticated malicious actor to execute administrative commands on a system via specially crafted HTTP or HTTPS requests.

CVE-2025-58034 is an OS Command Injection vulnerability (CWE-78: Improper Neutralization of Special Elements used in an OS Command ['OS Command Injection']) that may allow an authenticated attacker to execute unauthorized code on the underlying system via crafted HTTP requests or CLI commands.

Fortinet recommends affected organizations:

Apply the necessary upgrades listed in the table below and use Fortinet's guidance to address CVE-2025-64446.

Version
Affected
Solution

FortiWeb 8.0
8.0.0 through 8.0.1
Upgrade to 8.0.2 or above

FortiWeb 7.6
7.6.0 through 7.6.4
Upgrade to 7.6.5 or above

FortiWeb 7.4
7.4.0 through 7.4.9
Upgrade to 7.4.10 or above

FortiWeb 7.2
7.2.0 through 7.2.11
Upgrade to 7.2.12 or above

FortiWeb 7.0
7.0.0 through 7.0.11
Upgrade to 7.0.12 or above

Apply the necessary upgrades listed in the table below and use Fortinet's guidance to address CVE-2025-58034.

Version
Affected Solution

FortiWeb 8.0
8.0.0 through 8.0.1
Upgrade to 8.0.2 or above

FortiWeb 7.6
7.6.0 through 7.6.5
Upgrade to 7.6.6 or above

FortiWeb 7.4
7.4.0 through 7.4.10
Upgrade to 7.4.11 or above

FortiWeb 7.2
7.2.0 through 7.2.11
Upgrade to 7.2.12 or above

FortiWeb 7.0
7.0.0 through 7.0.11
Upgrade to 7.0.12 or above

If you cannot immediately upgrade the affected systems, disable HTTP or HTTPS for internet-facing interfaces. Note: Limiting access to HTTP/HTTPS management interfaces to internal networks is a best practice that reduces, but does not eliminate, risk; upgrading the affected systems remains essential and is the only way to fully remediate this vulnerability.

After upgrading, review configuration and review logs for unexpected modifications or the addition of unauthorized administrator accounts.

CISA added CVE-2025-64446 and CVE-2025-58034 to its Known Exploited Vulnerabilities (KEV) Catalog on Nov. 14, 2025 and Nov. 18, 2025, respectively.

Disclaimer

Note: This Alert may be updated to reflect new guidance issued by CISA or other parties. Organizations should report incidents and anomalous activity to CISA's 24/7 Operations Center at contact@cisa.dhs.gov or (888) 282-0870.

The information in this report is being provided "as is" for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.

Notes:

FortiGuard Labs, Path confusion vulnerability in GUI (November 14, 2025),

<https://fortiguard.fortinet.com/psirt/FG-IR-25-910>.

FortiGuard Labs, Multiple OS command injection in API and CLI (November 18, 2025),

<https://fortiguard.fortinet.com/psirt/FG-IR-25-513>.

<https://www.cisa.gov/news-events/alerts/2025/11/14/fortinet-releases-security-advisory-relative-path-traversal-vulnerability-affecting-fortiweb>