مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Fortinet FortiWeb

Tracking #:432318011

Date:15-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical zero-day path traversal vulnerability in Fortinet FortiWeb is being actively exploited in the wild. The flaw allows unauthenticated remote attackers to bypass authentication and execute administrative actions, including creating new admin users.

TECHNICAL DETAILS:

Fortinet has released a security advisory addressing a critical relative path traversal vulnerability (CVE-2025-64446) affecting multiple versions of its FortiWeb web application firewall (WAF) products. This vulnerability may allow an unauthenticated attacker to execute administrative commands on the affected system via specially crafted HTTP or HTTPS requests. Exploitation could result in complete compromise of the FortiWeb management interface. Fortinet has observed this vulnerability being actively exploited in the wild.

Vulnerability Details

- CVE-2025-64446
- CVSS Score 9.1 Critical
- A **path confusion / traversal vulnerability** within the FortiWeb GUI component. Attackers can send specially crafted HTTP/HTTPS POST requests to manipulated API paths, enabling authentication bypass and remote administrative command execution.
- Impact: Allows an attacker with no prior access to execute administrative commands, create administrator accounts, and gain full control over FortiWeb management functionality.
- A public proof-of-concept (PoC) exploit is available

Version	Affected Versions	Fixed Versions
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

RECOMMENDATIONS:

- Upgrade to the fixed versions immediately.
- Review system logs and configurations for unexpected changes.
- Temporary Mitigation (if immediate patching is not possible):
  - Disable HTTP/HTTPS access for all Internet-facing management interfaces.
  - Restrict management access to trusted internal networks only.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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