Security Advisory 2025-024

Critical Vulnerability in FortiWeb

2025-07-11 — v1.0

TLP:CLEAR

History:

- *11/07/2025 — v1.0 – Initial publication*

Summary

On July 8, 2025, Fortinet released a security advisory addressing a critical vulnerability in its FortiWeb product that would allow an attacker to execute unauthorised code or commands on the affected systems.

It is recommended mitigating this vulnerability as soon as possible.

Technical Details

The vulnerability **CVE-2025-25257**, with a CVSS score of 9.6, is due to an improper neutralisation of special elements used in an SQL command. It may allow an unauthenticated attacker to execute unauthorised SQL code or commands via crafted HTTP or HTTPs requests.

Affected Products

The following product versions are affected by the vulnerability:

- FortiWeb 7.6, versions 7.6.0 through 7.6.3
- FortiWeb 7.4, versions 7.4.0 through 7.4.7
- FortiWeb 7.2, versions7.2.0 through 7.2.10
- FortiWeb 7.0, versions 7.0.0 through 7.0.10

Recommendations

It is recommended updating affected devices as soon as possible.

Mitigation

It is possible to mitigate this vulnerability by disabling the HTTP/HTTPS administrative interface.

References

[1] https://fortiguard.fortinet.com/psirt/FG-IR-25-151