Health-ISAC
Collaborating for Resilience in Health

THREAT BULLETINS

A Critical FortiSIEM Flaw Was Disclosed with Exploit Code Available (CVE-2025-25256)

TLP:WHITE

Aug 13, 2025

On August 12, 2025, FortiGuard Labs issued an advisory on a critical FortiSIEM flaw, tracked as CVE-2025-25256. According to the advisory, a practical exploit code is available in the wild.

The flaw exists due to improper neutralization of special elements used in an OS command in FortiSIEM devices. In the event of successful exploitation, the flaw could allow threat actors to execute unauthorized code via crafted CLI requests. The flaw has a CVSS score of 9.8, highlighting its criticality.

Affected FortiSIEM versions are as follows:

- FortiSIEM 7.3: Versions 7.3.0 – 7.3.1
- FortiSIEM 7.2: Versions 7.2.0 – 7.2.5
- FortiSIEM 7.1: Versions 7.1.0 – 7.1.7
- FortiSIEM 7.0: Versions 7.0.0 – 7.0.3
- FortiSIEM 6.7: Versions 6.7.0 – 6.7.9
- All versions of 6.6, 6.5, 6.4, 6.3, 6.2, 6.1, and 5.4

Patches are available for vulnerable versions, and immediate patching is strongly recommended since the existence of exploit code increases the likelihood of attacks.

For organizations that are currently unable to apply patches, a temporary workaround is to limit access to the phMonitor port (7900).

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and take the necessary actions to ensure risk mitigations are implemented, including:

- Patch all vulnerable FortiSIEM devices.
- If patching is not possible, limit access to the phMonitor port (7900) as a temporary workaround.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patient Resources.

Reference(s)	securityonline, hhs, fortiguard

Sources
https://www.fortiguard.com/psirt/FG-IR-25-152

https://securityonline.info/fortisiem-cve-2025-25256-cvss-9-8-remote-unauthenticated-command-injection-with-exploit-in-the-wild/

Incident Date
Aug 12, 2025 (UTC)

Alert ID 29bd1577

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-25256, FortiSIEM

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**