ADVISORY !

SRI LANKA CERT|CC
SRI LANKA COMPUTER EMERGENCY READINESS TEAM

TLP : CLEAR DATE : 18th August 2025 REF NO : CERT-NCSOC-0236

Fortinet FortiSIEM Command Injection Vulnerability

Severity Level: CRITICAL

Components Affected

- FortiSIEM 5.4 - All version
- FortiSIEM 6.1-6.6 - All versions
- FortiSIEM 6.7 - 6.7.0 through 6.7.9
- FortiSIEM 7.0 - 7.0.0 through 7.0.3
- FortiSIEM 7.1 - 7.1.0 through 7.1.7
- FortiSIEM 7.2 - 7.2.0 through 7.2.
- FortiSIEM 7.3 - 7.3.0 through 7.3.1

WatchTowr Labs has detailed a severe **pre-authentication command injection vulnerability** in Fortinet FortiSIEM. This flaw lets unauthenticated attackers remotely execute arbitrary code or commands on vulnerable systems by sending crafted CLI requests, with no user involvement needed.

Description

The identified vulnerability includes:

- CVE-2025-25256 – A critical pre-authentication command injection vulnerability in Fortinet FortiSIEM systems (CVSS score: 9.8). The flaw is caused by improper neutralization of special elements used in OS command injection (CWE-78).
- The vulnerability exists in the phMonitor service (running on TCP port 7900), responsible for monitoring FortiSIEM processes and distributing tasks.

Impact

- Remote Code Execution (RCE) – Unauthenticated attackers can execute arbitrary commands.
- Full System Compromise – Exploitation allows attackers to take control of vulnerable FortiSIEM systems.
- Stealthy Exploitation – Exploitation attempts do not produce distinctive indicators of compromise, complicating detection and response.

Solution/ Workarounds

Recommended Actions:

- Patch immediately – Upgrade to the following fixed versions:
  - FortiSIEM 6.7 → Upgrade to 6.7.10 or above
  - FortiSIEM 7.0 → Upgrade to 7.0.4 or above
  - FortiSIEM 7.1 → Upgrade to 7.1.8 or above
  - FortiSIEM 7.2 → Upgrade to 7.2.6 or above
  - FortiSIEM 7.3 → Upgrade to 7.3.2 or above
  - FortiSIEM 5.4, 6.1–6.6 → All versions affected; migrate to supported releases

Temporary Mitigation (if patching is not possible):

- Restrict access to TCP port 7900 (phMonitor) to trusted internal hosts only.
- Monitor for suspicious system activity, although clear IoCs are lacking.

Reference

- https://labs.watchtowr.com
- https://cert.europa.eu
- https://cyber.gc.ca
- https://www.fortiguard.com/psirt

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.