POSTING DATE: 2026/01/16

[VULNERABILITY ALERT] Fortinet FortiSIEM Contains a Critical Security Vulnerability (CVE-2025-64155)

- Subject: [VULNERABILITY ALERT] Fortinet FortiSIEM Contains a Critical Security Vulnerability (CVE-2025-64155)

- Content Description:
    - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center Security Alert TWCERTCC-200-202601-00000010
    - FortiSIEM is Fortinet's next-generation Security Information and Event Management platform that utilizes AI and automation to enhance threat detection and security operations efficiency, reducing management complexity.
    - Recently, Fortinet released a critical security vulnerability announcement (CVE-2025-64155, CVSS: 9.8). This is an OS command injection vulnerability that may allow an unauthenticated attacker to execute unauthorized code or commands through specially crafted TCP requests.
- Affected Platforms:
    - FortiSIEM versions 6.7.0 to 6.7.10
    - FortiSIEM versions 7.0.0 to 7.0.4
    - FortiSIEM versions 7.1.0 to 7.1.8
    - FortiSIEM versions 7.2.0 to 7.2.6
    - FortiSIEM versions 7.3.0 to 7.3.4
    - FortiSIEM version 7.4.0
- Recommended Actions:
    - Please update to the following versions:
    - FortiSIEM version 7.1.9 (inclusive) or later
    - FortiSIEM version 7.2.7 (inclusive) or later
    - FortiSIEM version 7.3.5 (inclusive) or later
    - FortiSIEM version 7.4.1 (inclusive) or later
    - Note: For FortiSIEM versions 6.7 and 7.0, please migrate to a fixed version.
- Reference Material:
    1. https://www.twcert.org.tw/tw/cp-169-10632-91641-1.html

---

Computer and Communication Center
Network Systems Division, Respectfully

From:
https://net.nthu.edu.tw/netsys/ - 網路系統組

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260116_04

Last update: **2026/01/16 09:41**