

Posting date: 2025/08/18

[Vulnerability Alert]Fortinet's FortiSIEM has a major security vulnerability (CVE-2025-25256)

- Subject: [Vulnerability Alert]Fortinet's FortiSIEM has a major security vulnerability (CVE-2025-25256)
- Details:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202508-00000007
 - FortiSIEM is Fortinet's next-generation Security Information and Event Management platform, which uses AI and automation to enhance threat detection, improve security operation efficiency, and reduce management complexity. Recently, Fortinet issued a major security vulnerability announcement (CVE-2025-25256, CVSS: 9.8). This is an operating system command injection vulnerability that could allow an unauthenticated attacker to execute unauthorized code or commands through a specially crafted Command Line Interface (CLI) request.
- Affected Platforms:
 - FortiSIEM versions 7.3.0 to 7.3.1
 - FortiSIEM versions 7.2.0 to 7.2.5
 - FortiSIEM versions 7.1.0 to 7.1.7
 - FortiSIEM versions 7.0.0 to 7.0.3
 - FortiSIEM versions 6.7.0 to 6.7.9
- Recommended Actions:
 - Please update to the following versions:
 - FortiSIEM version 7.3.2
 - FortiSIEM version 7.2.6
 - FortiSIEM version 7.1.8
 - FortiSIEM version 7.0.4
 - FortiSIEM version 6.7.10
 - FortiSIEM versions 6.6 and earlier should be migrated to a fixed version
- References:
 - <https://www.twcert.org.tw/tw/cp-169-10322-f7c42-1.html>

Computer and Communications Center
Network Systems Group, Regards

From:

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

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250818_01



Last update: **2025/08/18 15:34**