Posted Date: 2025/10/22

[Vulnerability Alert] Fortinet FortiPAM and FortiSwitchManager have high-risk security vulnerability (CVE-2025-49201), please confirm and patch as soon as possible

- Subject: [Vulnerability Alert] Fortinet FortiPAM and FortiSwitchManager have high-risk security vulnerability (CVE-2025-49201), please confirm and patch as soon as possible
- Content:
 - Forwarded from National Information Security Information Sharing and Analysis Center NISAC-200-202510-00000158
 - Researchers have discovered a Weak Authentication vulnerability (CVE-2025-49201) in the GUI of Fortinet FortiPAM and FortiSwitchManager. An unauthenticated remote attacker can bypass the authentication process and log in to the system through brute-forcing, thereby executing unauthorized commands. Please confirm and patch as soon as possible.
- Affected Platforms:
 - FortiPAM version 1.5.0
 - FortiPAM versions 1.4.0 to 1.4.2
 - FortiPAM all 1.3 versions
 - FortiPAM all 1.2 versions
 - FortiPAM all 1.1 versions
 - FortiPAM all 1.0 versions
 - FortiSwitchManager versions 7.2.0 to 7.2.4
- Recommended Measures:
 - The official source has released a patch for the vulnerability; please refer to the official instructions for update at the following URL:
 - https://fortiguard.fortinet.com/psirt/FG-IR-25-010
- References:
 - 1. https://nvd.nist.gov/vuln/detail/CVE-2025-49201
 - 2. https://fortiguard.fortinet.com/psirt/FG-IR-25-010

Computer and Communications Center **Network Systems Group**

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

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251022 04

Last update: 2025/10/22 16:51

×

Last update: 2025/10/22 en:mailing:announcement:20251022_04 https://net.nthu.edu.tw/netsys/en:mailing:announcement:20251022_04