Posting Date: 2026/06/24

Vulnerability AlertFortinet Firewalls and Other Devices Targeted in Credential Theft Attacks; Please Verify and Patch Immediately

- Subject: Vulnerability AlertFortinet Firewalls and Other Devices Targeted in Credential Theft Attacks; Please Verify and Patch Immediately

- Description:
  - Forwarding National Information Security Analysis Center Security Alert NISAC-400-202606-00000006
  - Researchers have discovered that attackers are launching large-scale credential theft attacks against Fortinet firewalls, VPN appliances, and other devices. It is suspected that the attackers have obtained credential data for these devices, enabling them to bypass security defenses on a massive scale.
  - Please utilize the following lookup tool to verify whether your devices have been exposed, and implement remedial measures as soon as possible. Tool Link: https://www.hudsonrock.com/fortinet
- Affected Platforms:
  - All Fortinet devices
- Recommended Actions:
  1. Hide Management Interfaces: Promptly verify whether device management interfaces are exposed to the internet. Remove management interfaces from the public internet and restrict access to trusted IPs or via jump servers/VPNs only.
  2. Comprehensive Device Password Reset: Change all administrator passwords for Fortinet device management interfaces and VPNs immediately.
  3. Enable Multi-Factor Authentication (MFA): It is recommended to enable multi-factor authentication on all remote access and administrator accounts.
  4. Enforce Hashing Algorithm Upgrade: After upgrading FortiOS, require all administrators to log into the firewall at least once. The system will automatically upgrade the password encryption to the more secure PBKDF2 algorithm, making it harder to crack.
- Reference:
  1. https://www.hudsonrock.com/fortinet

Computer and Communication Center
Network Systems Division

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

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260624_22

Last update: **2026/06/24 16:25**