BREAKING CYBERSECURITY NEWS: Over 16,000 Fortinet DEVICES COMPROMISED WITH SYMLINK BACKDOOR

Vairav Cyber Security News Report

Date: April 17, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A significant cybersecurity incident has compromised over 16,000 Fortinet FortiGate devices worldwide. Attackers exploited previously patched vulnerabilities to install a symlink-based backdoor, granting persistent read-only access to sensitive system files. This technique allows unauthorized access even after devices have been updated, posing ongoing risks to affected organizations. The Shadowserver Foundation initially reported 14,000 compromised devices, with the number rising to 16,620 as of April 16, 2025.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Threat actors have employed a symlink-based persistence mechanism to maintain unauthorized access to FortiGate devices. By creating symbolic links in the language files directory, which is publicly accessible on devices with SSL-VPN enabled, attackers can access the root file system. This method allows them to retain read-only access even after the original vulnerabilities have been patched. The threat actors use the following vulnerabilities to gain initial access.

- **CVE-2022-42475**: Heap-based buffer overflow vulnerability assigned a CVSS score of 9.3 that impacts the following products
    - **FortiOS SSL-VPN**:
        - 7.2.0 through 7.2.2
        - 7.0.0 through 7.0.8
        - 6.4.0 through 6.4.10
        - 6.2.0 through 6.2.11
        - 6.0.15 and earlier
    - **FortiProxy SSL-VPN**:
        - 7.2.0 through 7.2.1
        - 7.0.7 and earlier

- **CVE-2023-27997:** Heap-based buffer overflow vulnerability assigned a CVSS score of 9.2 that impacts the following products:

- **FortiOS SSL-VPN:**
  - 7.2.4 and below
  - 7.0.11 and below
  - 6.4.12 and below
  - 6.0.16 and below
- **FortiProxy SSL-VPN:**
  - 7.2.3 and below
  - 7.0.9 and below
  - 2.0.12 and below
  - 1.2 (all versions)
  - 1.1 (all versions)

- **CVE-2024-21762:** Out-of-bounds write vulnerability assigned a CVSS score of 9.6 that impacts the following products
  - **FortiOS:**
    - 7.4.0 through 7.4.2
    - 7.2.0 through 7.2.6
    - 7.0.0 through 7.0.13
    - 6.4.0 through 6.4.14
    - 6.2.0 through 6.2.15
    - 6.0.0 through 6.0.17
  - **FortiProxy:**
    - 7.4.0 through 7.4.2
    - 7.2.0 through 7.2.8
    - 7.0.0 through 7.0.14
    - 2.0.0 through 2.0.13
    - 1.2.0 through 1.2.13
    - 1.1.0 through 1.1.6
    - 1.0.0 through 1.0.7

Identification: The Shadowserver Foundation detected the compromised devices through its threat monitoring platform. Fortinet had previously warned customers about this persistence mechanism, noting that it was linked to attacks dating back to 2023.

Affected Entities/Industries: The compromised devices are globally distributed, affecting various sectors, including government, healthcare, finance, and critical infrastructure. Organizations using FortiGate devices with SSL-VPN enabled are particularly at risk.

Potential Impact:

- Unauthorized access to sensitive system files
- Potential for data exfiltration
- Increased risk of further exploitation
- Challenges in detecting and removing the backdoor

Exploitation Methods: Attackers exploited known vulnerabilities, including CVE-2022-42475, CVE-2023-27997, and CVE-2024-21762, to gain initial access. They then created symbolic links in the language files directory to maintain persistent access.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Audit FortiGate devices for unauthorized symbolic links in the language files directory.
- Disable SSL-VPN if not essential.
- Apply the latest FortiOS updates and patches.
- Monitor network traffic for unusual activity related to FortiGate devices.

Security Best Practices

- Implement strict access controls and least privilege principles.
- Regularly review and update firewall and VPN configurations.
- Conduct periodic security assessments and vulnerability scans.

For Advanced Security Teams

- Develop custom detection rules to identify unauthorized symbolic links.
- Integrate threat intelligence feeds to stay informed about emerging threats.
- Collaborate with Fortinet support for in-depth analysis and remediation guidance.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.bleepingcomputer.com/news/security/over-16-000-fortinet-devices-compromised-with-symlink-backdoor/

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com