Fortinet Warns of Post-Exploitation Persistence via Symlinks in FortiGate VPNs

Overview

Fortinet is warning that some threat actors have found a post-exploitation technique which allows them to maintain persistent, unauthorized access to FortiGate VPN devices, even after organizations patch known vulnerabilities (CVE-2022-42475, CVE-2023-27997, and CVE-2024-21762).

This isn't a new vulnerability, but a case of attackers taking advantage of leftover artifacts from earlier compromises. Affected products include:

- FortiGate devices running FortiOS versions prior to 7.6.2, 7.4.7, 7.2.11, 7.0.17, and 6.4.16 with SSL-VPN enabled

The persistence technique exploits residual artifacts from previous compromises, specifically symlinks in the SSL-VPN's language directory that point to the root filesystem. These symlinks (shortcuts that point to other files) allow attackers to access sensitive files and configurations via the SSL-VPN interface. Fortinet has released updates to detect and remove the symlinks and is urging customers to double-check their systems for signs of tampering.

Aspire Protects

- **Patch –** Upgrade to FortiOS versions 7.6.2, 7.4.7, 7.2.11, 7.0.17, and 6.4.16. You may find patch guidance in Fortinet's advisory.
  - **Please note** that just patching the original CVEs isn't enough in this case. The symlink technique is something attackers used after they got in, and it can stick around even after updates.
  - If your FortiGate devices were compromised before, it's worth checking for leftover artifacts like symlinks that could still be giving attackers a way in. Fortinet's latest updates include checks to help detect and clean these up.
- Inspect the SSL-VPN's language directory for unauthorized symlinks pointing to the root filesystem.
- Reset credentials and certificates on potentially compromised devices.
- Implement real-time file system integrity checking to detect unauthorized modifications.

TTPs to Watch

Persistence

- Create or Modify System Process [T1543] – Attackers may create symlinks to maintain access.

Defense Evasion

- Masquerading [T1036] – Use of symlinks to disguise unauthorized access.

Initial Access

- Exploit Public-Facing Application [T1190] – Exploitation of known vulnerabilities in FortiGate devices.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability may impact any organization using FortiGate devices for remote access, but some industries face a higher risk due to how widely they rely on VPNs and how often they're targeted by threat actors.

- Healthcare
- Education
- Retail
- Finance
- Manufacturing
- Government
- Energy

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.

  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Analysis of Threat Actor Activity | Fortinet Blog

Real-time file system integrity checking | FortiGate / FortiOS 7.6.2 | Fortinet Document Library