Zero-Day Vulnerability in Fortinet Firewalls

Overview

Threat actors are actively exploiting a recently discovered authentication bypass zero-day vulnerability (CVE-2024-55591) in FortiOS and FortiProxy to hijack Fortinet firewalls and compromise enterprise networks. This vulnerability impacts FortiOS 7.0.0–7.0.16, FortiProxy 7.0.0–7.0.19, and FortiProxy 7.2.0–7.2.12.

Exploitation of this flaw allows attackers to gain super-admin privileges through malicious requests to the Node.js websocket module. Once exploited, attackers have been observed:

- Creating randomly generated admin or local accounts.
- Adding these accounts to SSL VPN user groups or creating new groups.
- Modifying firewall policies and configurations.
- Using rogue accounts to log in to SSL VPNs for lateral movement within networks.

Arctic Wolf Labs discovered the campaign targeting Fortinet FortiGate firewalls with publicly exposed management interfaces. The campaign has been traced back to mid-November 2024 and follows four distinct phases:

1. Vulnerability Scanning (November 16–23, 2024)
2. Reconnaissance (November 22–27, 2024)
3. SSL VPN Configuration (December 4–7, 2024)
4. Lateral Movement (December 16–27, 2024)

The threat actors exploited the zero-day vulnerability to gain unauthorized access, manipulate configurations, and create new accounts for further exploitation. While Arctic Wolf initially discovered the activity, Fortinet confirmed the existence of the vulnerability on January 14, 2025.

Aspire Protects

- **Patch –** Fortinet released patches for CVE-2024-55591, which can be found in the company's security advisory.
    - Arctic Wolf published security bulletin with a warning of observed activity in this campaign.
- Arctic Wolf also recommends the following**:**

    - Disable Public Access - Immediately block public access to firewall management interfaces.
    - Limit Admin Access - Restrict access to trusted internal users only.
    - Check for Suspicious Changes - Audit admin accounts, VPN configurations, and recent system changes.
- To see other Aspire Emergency Flash Notice's, please visit Aspire's Managed Services Customer Portal.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attackers likely exploited exposed management interfaces.

Credential Access

- DCSync [T1003.006] – Threat actors extracted credentials for lateral movement.

Privilege Escalation

- Create or Modify Accounts [T1136] – New admin and local user accounts were added for VPN access.

Defense Evasion

- Modify System Configuration [T1496] – Attackers changed settings to avoid detection.

IoCs

IPv4 Address

- 23.27[.]140[.]65
- 66.135[.]27[.]178
- 157.245[.]3[.]251
- 45.55[.]158[.]47
- 167.71[.]245[.]10
- 137.184[.]65[.]71
- 155.133[.]4[.]175
- 31.192[.]107[.]165
- 37.19[.]196[.]65
- 64.190[.]113[.]25

Targeted Industries

Based on the usage of Fortinet FortiGate firewalls, potential industries could include

- Healthcare
- Finance
- Education
- Manufacturing
- Government
- Small to Medium Sized Businesses (SMBs)

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

Arctic Wolf Observes Targeting of Publicly Exposed Fortinet Firewall Management Interfaces | Arctic Wolf

Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls - Arctic Wolf

Snoops exploited Fortinet firewalls with 'probable' 0-day • The Register

Knowledge Base - Customer Support