Exploitation of DoS Vulnerability in Palo Alto Networks Firewalls

Overview

Palo Alto Networks has reported active exploitation of a Denial of Service (DoS) vulnerability, CVE-2024-3393, targeting PAN-OS software. This flaw allows unauthenticated attackers to send crafted packets that force firewalls to reboot.

CVE-2024-3393 is a Denial of Service (DoS) flaw affecting the DNS Security logging feature in Palo Alto Networks' PAN-OS software. Exploiting this vulnerability causes firewalls to reboot, interrupting their security functions.

Affected Products

- Vulnerable Versions
    - PAN-OS 11.2 (<11.2.3)
    - PAN-OS 11.1 (<11.1.5)
    - PAN-OS 10.2 (10.2.8–10.2.13)
    - PAN-OS 10.1 (10.1.14)
    - PAN-OS 11.0 (End of Life - no patch available)
- Unaffected Versions: PAN-OS 10.1.15, 10.2.14, 11.1.5, 11.2.3, and later.

Repeated exploitation of this vulnerability can place devices into maintenance mode, requiring manual intervention for recovery. This creates an opportunity for attackers to bypass defenses and launch further attacks. Due to exploitation, Aspire recommends patching immediately.

Aspire Protects

- **Patch –** Update affected systems to the latest patched PAN-OS versions - 10.1.15, 10.2.14, 11.1.5, or 11.2.3. You may find patch guidance in Palo Alto's advisory.
- If updates cannot be applied, disable DNS Security logging using the steps provided by Palo Alto Networks.
    - For unmanaged devices or devices managed by Panorama
        - Navigate to Objects > Security Profiles > Anti-spyware > DNS Policies, and set Log Severity to "none" for all DNS Security categories.
    - For Prisma Access
        - Submit a support case to disable DNS Security logging or expedite an upgrade.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Attackers send malicious packets via the network to exploit the firewall's DNS Security feature.

Impact

- Service Stop (T1489) – Repeated exploits result in denial of service, disrupting the firewall's availability.

IoCs

There are no known IoCs associated with CVE-2024-3393 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 Palo Alto vulnerability could impact a range of industries that rely on Palo Alto Networks firewalls. Key industries include:

- Finance
- Retail
- Energy and Utilities
- Government
- And others

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

CVE-2024-3393 PAN-OS: Firewall Denial of Service (DoS) in DNS Security Using a Specially Crafted Packet