NCA-05.041624: NCERT Advisory – PAN-OS Firewall Zero-Day Vulnerability

Introduction

The National Computer Emergency Response Team (NCERT) advises regarding a critical vulnerability impacting Palo Alto Networks' PAN-OS firewall. This vulnerability, tracked as CVE-2024-3400, presents a severe risk as it allows unauthenticated attackers to execute arbitrary code with root privileges on affected firewalls. The exploitation of this vulnerability has been observed in active attacks. The severity score assigned to this vulnerability is the maximum, 10.0.

Impact

Exploitation of CVE-2024-3400 could result in severe compromization of affected systems, potentially leading to unauthorized access, data breaches, and system manipulation by malicious actors.

Affected Systems and Devices

The vulnerability affects specific versions of PAN-OS software when both the GlobalProtect gateway and device telemetry features are enabled. The vulnerable versions are PAN-OS 10.2, 11.0, and 11.1.

Recommendations

1. **Apply Security Updates:** Ensure prompt application of security updates provided by Palo Alto Networks. Fixes for all the affected versions are expected by April 19, 2024. For now, implement the following hotfixes:

   - PAN-OS 10.2.9-h1
   - PAN-OS 10.2.8-h3
   - PAN-OS 10.2.7-h8
   - PAN-OS 10.2.5-h6
   - PAN-OS 10.2.3-h13
   - PAN-OS 10.2.1-h2
   - PAN-OS 11.0.4-h1
   - PAN-OS 11.0.3-h10
   - PAN-OS 11.1.2-h3
   - PAN-OS 11.1.1-h1
   - PAN-OS 11.1.0-h3

1. **Mitigate Immediately:** Until security updates are applied, implement the following mitigations:

PKCERT

   - Activate 'Threat ID 95187' for users with an active 'Threat Prevention' subscription to block attacks.
   - Configure vulnerability protection on 'GlobalProtect Interfaces' to prevent exploitation.
   - Disable device telemetry until patches are applied.

2. **<u>Follow Best Practices</u>:** Implement best practices for network security and firewall management. Regularly review and update security configurations to mitigate potential vulnerabilities.
3. **<u>Monitor and Respond</u>:** Continuously monitor network activity for any signs of exploitation or suspicious behavior. Have response plans in place to address any security incidents promptly.

References

1. Palo Alto Networks Security Advisory: Link
2. CISA Known Exploited Vulnerabilities (KEV) catalog: Link

NCERT urges to prioritize the implementation of these recommendations to safeguard systems against potential exploitation of CVE-2024-3400.

PKCERT