Palo Alto Firewalls Under Active Exploitation – CVE-2024-3400

Overview

Palo Alto Networks has recently confirmed the existence of proof-of-concept techniques that allow attackers to maintain persistence on compromised Palo Alto firewalls even after exploiting CVE-2024-3400 (CVSS 10) and performing system resets or upgrades.

Initially reported on April 12, 2024, this critical vulnerability, which allows unauthenticated command execution with root privileges, has been linked to a series of attacks potentially orchestrated by a state-sponsored threat actor. The exploitation involved a combination of an unassigned arbitrary file creation vulnerability and CVE-2024-3400, affecting PAN-OS versions across multiple devices.

Customers are advised to apply the provided patches, which address both the initial exploit and the following persistence techniques. Disabling device telemetry, previously suggested as a mitigation measure, is no longer effective. Palo Alto Networks has recommended enhanced factory resets for devices potentially compromised by these persistence techniques and urges customers to consult their support team to schedule this procedure.

Aspire Protects

- Since the vulnerability's disclosure, Palo Alto Networks has been actively updating its security advisories and expanding the range of affected PAN-OS versions.
- **Patch**
  - Upgrade to the fixed PAN-OS versions to address CVE-2024-3400. Ensure that updates are applied to PAN-OS versions 10.2.9-h1, 11.0.4-h1, and 11.1.2-h3, as well as any later releases.
  - Verify and apply all available hotfixes for affected PAN-OS versions, including 10.2.0-h3 through 10.2.9-h1, and 11.0.0-h3 through 11.0.4-h2.
- If you have not applied PAN-OS fixes or Threat Prevention signatures before April 25, 2024, or if there is a concern about persistent risks, schedule an enhanced factory reset through Palo Alto Networks Customer Support (TAC). This procedure helps ensure the device is clean from any potential persistent threats.
- Implement Threat Prevention signatures with IDs 95187, 95189, and 95191, available in Applications and Threats content version 8836-8695 and later. Monitor Palo Alto's advisory and new Threat Prevention content updates for additional Threat Prevention IDs around CVE-2024-3400.
- If any exploitation was observed on a device, please take the remediation steps suggested here: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA14u000000CrO6CAK
- For any questions, please reach out to Aspire's Customer Success Management team.

IoCs

IP Addresses

- 198[.]58[.]109[.]149
- 144[.]172[.]79[.]92
- 172[.]233[.]228[.]93
- 71[.]9[.]135[.]100
- 89[.]187[.]187[.]69

File Hashes

- 3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac
- 35a5f8ac03b0e3865b3177892420cb34233c55240f452f00f9004e274a85703c
- 755f5b8bd67d226f24329dc960f59e11cb5735b930b4ed30b2df77572efb32e8
- adba167a9df482aa991faaa0e0cde1182fb9acfbb0dc8d19148ce634608bab87
- c1a0d380bf55070496b9420b970dfc5c2c4ad0a598083b9077493e8b8035f1e9
- fe07ca449e99827265ca95f9f56ec6543a4c5b712ed50038a9a153199e95a0b7
- 96dbec24ac64e7dd5fef6e2c26214c8fe5be3486d5c92d21d5dcb4f6c4e365b9
- 448fbd7b3389fe2aa421de224d065cea7064de0869a036610e5363c931df5b7c
- e315907415eb8cfcf3b6a4cd6602b392a3fe8ee0f79a2d51a81a928dbce950f8
- 161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6

TTPs to Watch

- Tactic: Initial Access (TA0001)
  - Exploit Public-Facing Application (T1190) - Attackers may exploit the command injection vulnerability in PAN-OS's GlobalProtect portal or gateway to gain initial access to the target firewall.
- Tactic: Execution (TA0002)
  - Exploitation for Client Execution (T1203) - The attacker leverages the CVE-2024-3400 vulnerability to execute arbitrary code with root privileges on the affected firewall.
- Tactic: Persistence (TA0003)
  - Boot or Logon Autostart Execution (T1547) - Post-exploit persistence techniques may be used to survive system reboots and firmware upgrades, ensuring continued unauthorized access.
- Tactic: Privilege Escalation (TA0004)
  - Exploitation for Privilege Escalation (T1068) - The vulnerability allows attackers to escalate privileges to root, allowing them to take full control of the compromised firewall.

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 cyberattacks.
- **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

threat-intel/2024/2024-04-12 Palo Alto Networks GlobalProtect/indicators/iocs.csv at main · volexity/threat-intel · GitHub

Palo Alto firewalls: CVE-2024-3400 exploitation and PoCs for persistence after resets/upgrades - Help Net Security

CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect (paloaltonetworks.com)

Palo Alto Networks warns firewall exploits are spreading | Cybersecurity Dive