THREAT BULLETINS

Palo Alto PAN-OS Firewall Flaw CVE-2025-0111 Used in Exploit Chaining Attacks

TLP:WHITE

Feb 21, 2025

Palo Alto recently disclosed that PAN-OS firewalls vulnerable to CVE-2025-0111 are being used in exploit chain attacks.

In these attacks, CVE-2025-0111 is chained with CVE-2025-0108 and CVE-2024-9474, for which Palo Alto released patches in February 2025 and November 2024, respectively.

Despite fixes also being released for CVE-2025-0111 in February 2025, Palo Alto updated a previously distributed advisory after observing threat actors chaining it with CVE-2025-0108 and CVE-2024-9474 in exploit attempts on unpatched and unsecured PAN-OS web management interfaces.

Successful exploitation of CVE-2025-0111 allows unauthenticated threat actors with network access to the management web interface to read files on the PAN-OS filesystem that are readable by the “nobody” user. Health-ISAC previously released an alert in which threat actors were chaining CVE-2025-0108 and CVE-2024-9474 to exploit vulnerable PAN-OS firewalls.

CVE-2025-0108 is a PAN-OS flaw that allows unauthenticated attackers with network access to bypass authentication, potentially compromising the system's integrity and confidentiality. When

chained with other flaws, it could also lead to remote code execution. The flaw has a CVSS score of 7.8. Health-ISAC previously distributed a Vulnerability Bulletin alerting members about the flaw's existence.

Conversely, CVE-2024-9474 is a privilege escalation flaw in PAN-OS that allows a PAN-OS administrator to execute commands on firewalls with root privileges.

This alert is being shared to raise awareness of exploit-chaining attempts targeting vulnerable PAN-OS firewalls. It is a call to action to ensure patches are being applied as threat actors continue to discover ways to circumvent fixes provided by Palo Alto.

Recommendations:

- Apply available patches for vulnerable Palo Alto PAN-OS devices.
- Enforce network segmentation and strict network access control policies.
- Implement multi-factor authentication for accounts across the organization.
- Continuously monitor for suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	HHS, Health-ISAC Threat Advisory System, Health-ISAC Threat Advisory System, Palo Alto Networks, Infosecurity Magazine, Bleeping Computer, Security Affairs

Sources
https://security.paloaltonetworks.com/CVE-2025-0111
https://www.bleepingcomputer.com/news/security/palo-alto-networks-tags-new-firewall-bug-as-exploited-in-attacks/

https://securityaffairs.com/174409/hacking/palo-alto-networks-cve-2025-0111-actively-exploited.html
https://www.infosecurity-magazine.com/news/hackers-chain-exploits-three-palo/

Incident Date
Feb 21, 2025 (UTC)

Alert ID bbdf4651

View Alert

Share Feedback

was this helpful? |

Tags CVE-2025-0111, CVE-2025-0108, CVE-2024-9474, Palo Alto Networks

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**