THREAT BULLETINS

Palo Alto Networks Reports on the Exploitation of a New Flaw CVE-2024-3393

TLP:WHITE

Dec 27, 2024

On December 27, 2024, Palo Alto Networks disclosed a high-severity vulnerability, tracked as CVE-2024-3393, in its PAN-OS software that affects the DNS Security feature. According to the advisory, the flaw has already been exploited.

This flaw allows unauthenticated attackers to send malicious DNS packets, potentially causing Denial of Service (DoS) disruptions and forcing firewalls into maintenance mode. The company said it has reports of some of its customers already experiencing DoS when the firewall attempts to block the malicious DNS packets.

The vulnerability's CVSS score is 8.7, indicating high severity. The flaw is especially dangerous because it requires no user interaction or elevated privileges. Threat actors can exploit the flaw by sending the malicious DNS package to the vulnerable firewall, causing the crash and reboot of the system, and, in some cases, may result in Denial of Service. However, for the attack to be successful, the DNS feature must be enabled.

The flaw is affecting PAN-OS version 10. X and 11. X, including Prisma Access.

Health-ISAC advises members to upgrade to patched PAN-OS versions urgently to mitigate this risk. If patching is not possible, Palo

Alto Networks recommends setting DNS Security log severity to “none” as a temporary workaround.

Recommendations:

- Apply available patches for vulnerable Palo Alto devices.
- Ensure all of the devices are patched in a timely manner.
- Enforce network segmentation and strict network access control policies.
- Continuously monitor for suspicious activities.
- Have an incident response plan ready to limit operational disruptions in the event of a successful attack.
- Review the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients resources.

Reference(s)	Palo Alto Networks, HHS, The Hacker News, socradar

Sources
Palo Alto Networks Security Advisories
Palo Alto Releases Patch for PAN-OS DoS Flaw — Update Immediately
Severe Vulnerability in Palo Alto Networks PAN-OS Exposes Firewalls to Denial of Service (CVE-2024-3393)

Incident Date
Dec 27, 2024 (UTC)

Alert ID f9d58073

View Alert

Share Feedback
was this helpful? |

Tags CVE-2024-3393, Palo Alto PAN-OS

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

Share Threat Intel
For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

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/**