THREAT BULLETINS

Palo Alto Networks Critical Expedition Flaw CVE-2024-5910 Is Being Exploited

TLP:WHITE

Nov 08, 2024

On Thursday, November 7, 2024, Palo Alto Networks updated the security advisory for the critical vulnerability, CVE-2024-5910, to reflect the reported exploitation of the flaw.

The flaw, CVE-2024-5910, originally disclosed in July, is a missing authentication flaw that affects Palo Alto Networks' Expedition, a firewall configuration migration tool. In the event of a successful attack, the flaw could allow threat actors with network access to gain control of an Expedition admin account. As a result, threat actors can gain access to configuration settings, credentials, and other potentially sensitive data imported into vulnerable Expedition instances. The flaw's CVSS score is 9.3.

Given the widespread use of Palo Alto Networks devices among the membership, Health-ISAC advises network administrators to prioritize patching this vulnerability in cases where this has not already been done as the most efficient way to mitigate the threat of exploitation. Additionally, it is advised to continuously monitor systems for suspicious activity to prevent possible intrusion.

Recommendations:

- Apply available patches for vulnerable Palo Alto Networks devices.

- 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)	The Hacker News, HHS, Palo Alto Networks, Help Net Security

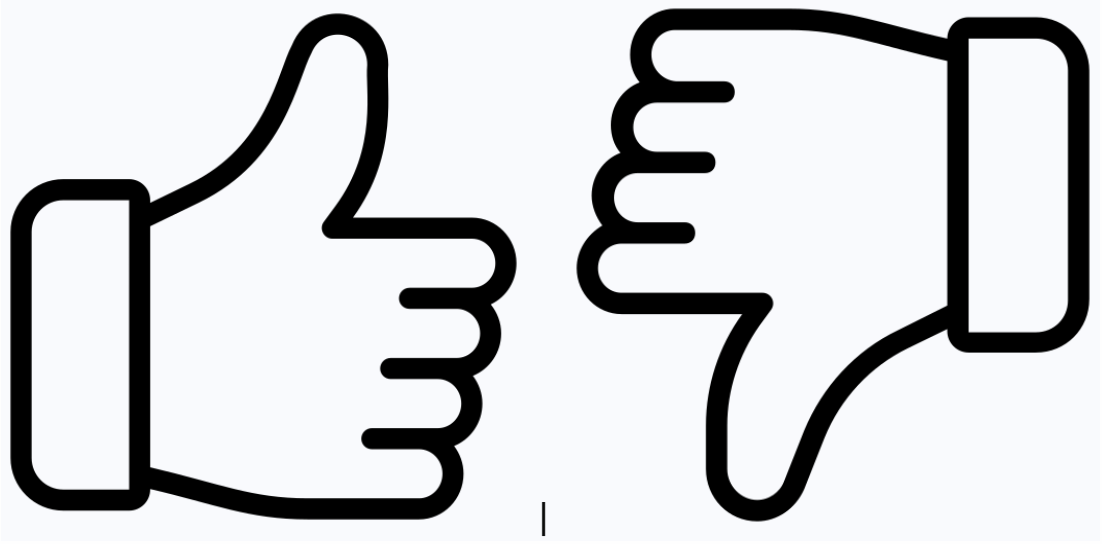
Sources
Palo Alto's Security Advisory
CISA Alerts to Active Exploitation of Critical Palo Alto Networks Vulnerability
Critical Palo Alto Networks Expedition bug exploited (CVE-2024-5910)

Incident Date
Nov 08, 2024 (UTC)

Alert ID 40410f9f

View Alert

Share Feedback
was this helpful?



Tags CVE-2024-5910, Palo Alto Networks

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/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.