Command Injection Vulnerability in PaloAlto PAN-OS

2024-09-16 — v1.0

TLP:CLEAR

History:

- *16/09/2024 — v1.0 – Initial publication*

Summary

On September 11, 2024, a high-severity command injection vulnerability has been addressed in PaloAlto PAN-OS. If exploited, this flaw could allow an authenticated attacker to execute arbitrary commands as root on the firewall.

Technical Details

The vulnerability **CVE-2024-8686**, with a CVSS score of 8.6, is a command injection vulnerability in Palo Alto Networks PAN-OS software. It enables an authenticated administrator to bypass system restrictions and run arbitrary commands as root on the firewall.

Affected Products

This vulnerability affects PAN-OS version 11.2.2.

Recommendations

CERT-EU strongly recommends updating affected PAN-OS installations to the latest version [1].

References

[1] https://security.paloaltonetworks.com/CVE-2024-8686