Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Zero-Day PAN-OS Flaws Exposing Systems to Full Control

Date of Publication	Admiralty Code	TA Number
November 19, 2024	A1	TA2024436

Summary

First Seen: November 2024
Affected Products: Palo Alto Networks PAN-OS software
Impact: Palo Alto Networks has issued critical security updates to address two actively exploited zero-day vulnerabilities, CVE-2024-0012 and CVE-2024-9474, in its PAN-OS software. These flaws, currently being exploited in the wild, pose significant risks, emphasizing the urgency for immediate patch application to safeguard affected systems.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-0012	Palo Alto Networks PAN-OS Management Interface Authentication Bypass Vulnerability	Palo Alto Networks PAN-OS software	✓	✓	✓
CVE-2024-9474	Palo Alto Networks PAN-OS Management Interface OS Command Injection Vulnerability	Palo Alto Networks PAN-OS software	✓	✓	✓

Vulnerability Details

#1

Palo Alto Networks has released critical security updates to address two zero-day vulnerabilities in its PAN-OS software namely CVE-2024-0012 and CVE-2024-9474, both of which are being exploited. CVE-2024-0012 can be chained with privilege escalation flaws like CVE-2024-9474, significantly increasing the risk of full system compromise. The exploitation of CVE-2024-0012 has been linked to a targeted campaign dubbed Operation Lunar Peek, underscoring the strategic and sophisticated nature of the attacks.

#2 CVE-2024-0012 is an authentication bypass vulnerability that allows unauthenticated attackers with network access to the management web interface to gain administrative privileges. This access can be used to alter configurations, perform administrative tasks, and exploit additional vulnerabilities, including CVE-2024-9474. CVE-2024-9474, a privilege escalation vulnerability, enables PAN-OS administrators to perform root-level actions on the firewall, giving attackers potential full control over the system.

#3 Post-exploitation activities linked to these vulnerabilities include interactive command execution and deploying malware, such as webshells, onto compromised firewalls. Organizations are strongly urged to patch these flaws immediately and bolster their overall security defenses to mitigate potential risks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-0012	Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1, Versions Prior to 11.0.6-h1, Versions Prior to 10.2.12-h2	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	CWE-306
CVE-2024-9474	Palo Alto Networks PAN-OS Versions Prior to 11.2.4-h1, Versions Prior to 11.1.5-h1 Versions Prior to 11.0.6-h1 Versions Prior to 10.2.12-h2, Verions Prior to 10.1.14-h6	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply Patches : Ensure all PAN-OS devices are promptly updated to the latest security versions to address CVE-2024-0012 and CVE-2024-9474. These vulnerabilities are fixed in PAN-OS 10.2.12-h2, PAN-OS 11.0.6-h1, PAN-OS 11.1.5-h1, PAN-OS 11.2.4-h1, and all subsequent PAN-OS versions. Applying these patches is crucial to securing your network against exploitation.

Restrict Access: Limit access to the PAN-OS management interface by only allowing trusted IP addresses or using VPNs for remote access to mitigate unauthorized exposure.

Least Privilege: Adhere to the idea of "least privilege" by giving users only the essential permissions they need for their tasks, restrict the access to the trusted parties only.

Vulnerability Management: Implement a robust vulnerability management process to ensure that software and systems are regularly assessed for vulnerabilities and updated with the required security patches. Prioritize critical vulnerabilities identified by security advisories and vendors to mitigate the risk of exploitation by threat actors.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0004 Privilege Escalation	TA0006 Credential Access	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1588.005 Exploits	T1556 Modify Authentication Process	T1068 Exploitation for Privilege Escalation

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	91[.]208[.]197[.]167 136[.]144[.]17[.]146 136[.]144[.]17[.]149 136[.]144[.]17[.]154 136[.]144[.]17[.]161 136[.]144[.]17[.]164 136[.]144[.]17[.]166 136[.]144[.]17[.]167 136[.]144[.]17[.]170 136[.]144[.]17[.]176 136[.]144[.]17[.]177 136[.]144[.]17[.]178 136[.]144[.]17[.]180 173[.]239[.]218[.]251 209[.]200[.]246[.]173 209[.]200[.]246[.]184 216[.]73[.]162[.]69 216[.]73[.]162[.]71 216[.]73[.]162[.]73 216[.]73[.]162[.]74
SHA256	3C5F9034C86CB1952AA5BB07B4F77CE7D8BB5CC9FE5C029A32C72ADC7E814668

Patch Details

Palo Alto Networks has addressed the vulnerabilities in recent updates. To secure your systems, upgrade to one of the listed patched versions or the latest available PAN-OS release.
CVE-2024-9474: Fixed in PAN-OS 10.1.14-h6, 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1, and all later versions.
CVE-2024-0012: Fixed in PAN-OS 10.2.12-h2, 11.0.6-h1, 11.1.5-h1, 11.2.4-h1, and all later versions.

Links:
https://docs.paloaltonetworks.com/pan-os/11-2/pan-os-release-notes/pan-os-11-2-4-known-and-addressed-issues/pan-os-11-2-4-addressed-issues-

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-release-notes/pan-os-11-1-5-known-and-addressed-issues/pan-os-11-1-5-addressed-issues,-

https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-release-notes/pan-os-10-2-12-known-and-addressed-issues/pan-os-10-2-12-h1-addressed-issues

https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-release-notes/pan-os-10-1-14-known-and-addressed-issues/pan-os-10-1-14-h4-addressed-issues

References

https://security.paloaltonetworks.com/CVE-2024-0012

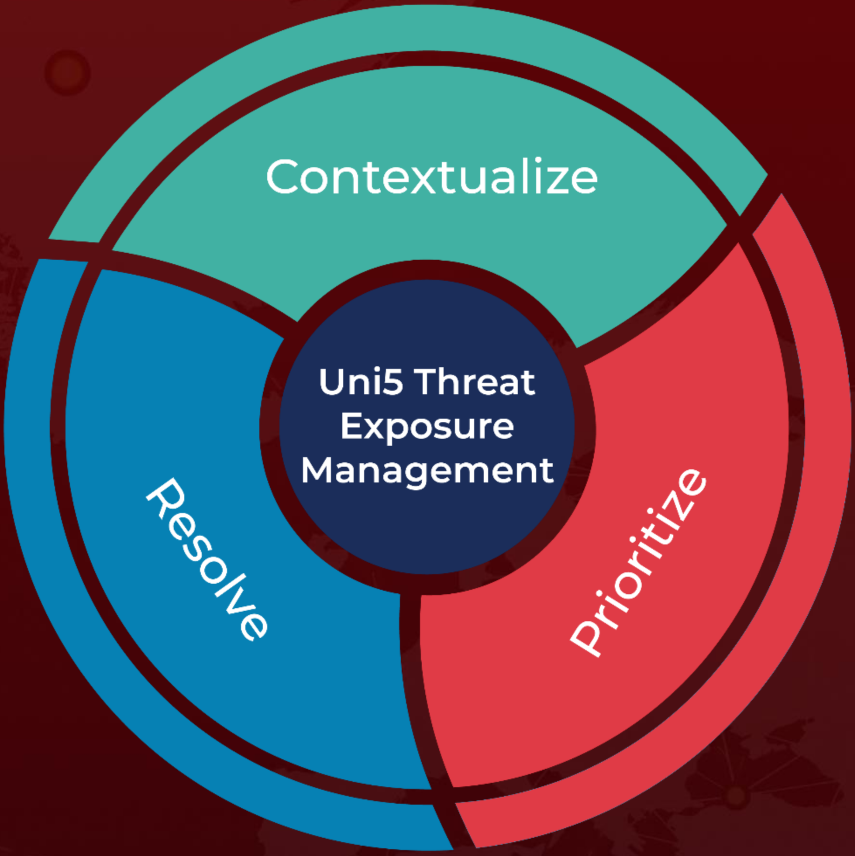
https://security.paloaltonetworks.com/CVE-2024-9474

https://unit42.paloaltonetworks.com/cve-2024-0012-cve-2024-9474/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

November 19, 2024 • 7:00 AM

More at www.hivepro.com