

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Hackers Exploiting Critical Palo Alto Networks Vulnerability

Date of Publication

November 8, 2024

Admiralty Code

A1

TA Number

TA2024421

Summary

First Seen: July 10, 2024

Affected Product: Palo Alto Expedition

Impact: A critical vulnerability in Palo Alto Networks' Expedition tool, identified as CVE-2024-5910, which allows attackers to exploit a missing authentication function to take over admin accounts. This vulnerability can lead to unauthorized access to sensitive data and can be chained with another flaw for further exploitation. Administrators are advised to restrict access and rotate credentials after applying the necessary updates.

⚙️ CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-5910	Palo Alto Expedition Missing Authentication Vulnerability	Palo Alto Expedition	✗	✓	✓
CVE-2024-9464	Palo Alto Expedition OS command injection Vulnerability	Palo Alto Expedition	✗	✗	✓

Vulnerability Details

#1

A critical vulnerability in Palo Alto Networks' Expedition tool, identified as CVE-2024-5910, poses a significant risk by allowing attackers with network access to exploit a missing authentication function. This flaw enables attackers to potentially take over Expedition admin accounts and gain unauthorized access to sensitive configuration data, credentials, and other critical information.

#2

The flaw is characterized by the absence of an authentication requirement for a crucial function within Expedition. This means that attackers can remotely reset admin credentials on servers that are exposed to the Internet. If successfully exploited, this could enable attackers to gain control over the Expedition admin account, posing severe risks as they could access configuration secrets and other sensitive data stored within the system.

#3

Moreover, this vulnerability can be chained with another recently patched flaw, CVE-2024-9464, which is a command injection vulnerability. This chaining capability allows attackers to execute arbitrary commands without authentication on vulnerable servers, further amplifying the threat landscape.

#4

In conclusion, the ongoing exploitation of this vulnerability underscores the importance of prompt updates and security measures for organizations using Palo Alto Networks' Expedition tool. Administrators are urged to act swiftly to mitigate potential risks associated with this critical flaw and ensure the security of their systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-5910	Palo Alto Networks' Expedition versions prior to 1.2.92	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*	CWE-306
CVE-2024-9464	Palo Alto Networks' Expedition versions prior to 1.2.96	cpe:2.3:a:paloaltonetworks:expedition:*:*:*:*:*:*	CWE-78

Recommendations



Upgrade Software: Upgrade Expedition to version 1.2.92 or later to address the identified vulnerabilities. This update is crucial to patch the missing authentication mechanism that allows attackers to bypass normal security checks.



Restrict Network Access: If immediate upgrading is not feasible, limit network access to the Expedition tool strictly to authorized users, hosts, or networks. This reduces the attack surface and minimizes the risk of unauthorized exploitation.



Credential Management: After upgrading, immediately rotate all usernames, passwords, and API keys associated with Expedition, including those for any integrated firewalls or devices. This ensures that any potentially compromised credentials are no longer valid.



Implement Network Monitoring and Alerting: Monitor Expedition for unusual activity, such as unauthorized login attempts or unexpected changes to administrative settings. Enhanced monitoring can help detect and respond quickly to any potential exploitation attempts. Logging and alerting should also be configured to provide timely notifications of suspicious activity on the network.



Conduct Security Audits and Vulnerability Scans: Regularly audit your infrastructure for security vulnerabilities, especially on critical management tools like Expedition. Employing vulnerability scanners can help detect unpatched or misconfigured systems. These checks are essential to maintaining an effective security posture.



Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0042</u> Resource Development	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation
<u>T1059</u> Command and Scripting Interpreter	<u>T1588.006</u> Vulnerabilities	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1078</u> Valid Accounts		



Patch Details

Upgrade Palo Alto Networks' Expedition version to 1.2.96 or later.

Link:

<https://live.paloaltonetworks.com/t5/expedition-release-notes/expedition-1-2-96-hotfix-information/ta-p/599340>



References

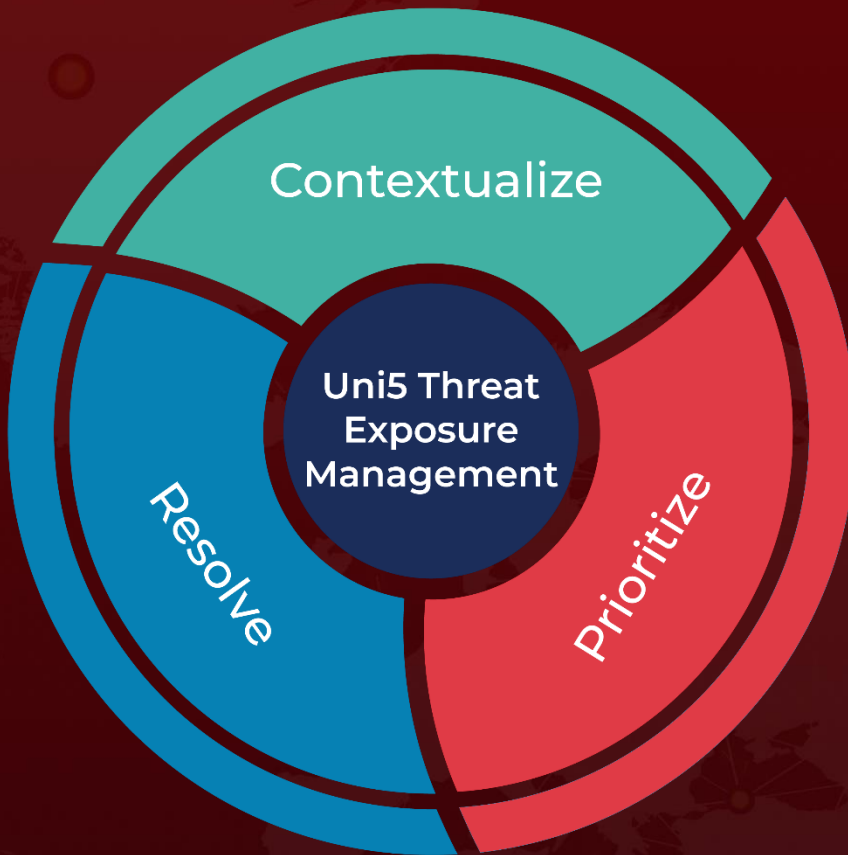
<https://security.paloaltonetworks.com/CVE-2024-5910>

<https://security.paloaltonetworks.com/PAN-SA-2024-0010>

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 7, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com