Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

PAN-OS Flaw Exploited Causing Firewall Crashes

Date of Publication	Admiralty Code	TA Number
December 27, 2024	A1	TA2024475

Summary

First Seen: December 2024
Affected Products: Palo Alto Networks PAN-OS
Impact: Palo Alto Networks has revealed a high-severity vulnerability, CVE-2024-3393, affecting its PAN-OS software. This Denial-of-Service (DoS) flaw resides in the DNS Security feature, enabling an unauthenticated attacker to exploit it by sending crafted packets through the firewall's data plane. When triggered, this attack forces the firewall to reboot, and repeated exploitation can push the system into maintenance mode, disrupting operations.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-3393	Palo Alto Networks Denial of Service (DoS) Vulnerability	Palo Alto Networks PAN-OS	✗	✗	✓

Vulnerability Details

#1

CVE-2024-3393 is a high severity Denial-of-Service (DoS) vulnerability identified in the DNS Security feature of Palo Alto Networks' PAN-OS software. This flaw enables an unauthenticated attacker to send specially crafted packets through the firewall's data plane, causing it to crash and reboot. Repeated exploitation can force the firewall into maintenance mode, severely impacting operations.

#2 The issue arises from improper handling of exceptional conditions within the DNS Security feature. Attackers exploit this weakness by injecting malicious packets that disrupt the firewall's normal functioning. The vulnerability has confirmed being exploited in real-world, with attackers successfully triggering DoS conditions in production environments.

#3 To address this risk, Palo Alto Networks strongly recommends upgrading to the latest secure versions of PAN-OS. Prisma Access users will receive updates in two phases during the weekends of January 3rd and January 10th, 2024. Prompt action is advised to safeguard critical infrastructure against this active threat.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-3393	PAN-OS 11.2: Versions below 11.2.3; PAN-OS 11.1: Versions below 11.1.5; PAN-OS 10.2: Versions upto 10.2.8, Versions below 10.2.10-h12 and Versions below 10.2.13-h2; PAN-OS 10.1: Versions upto 10.1.14 and Versions below 10.1.14-h8	cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*	CWE-754

Recommendations

Upgrade: To mitigate the vulnerability, promptly update your Palo Alto Networks firewalls by installing the patched versions. Ensure you upgrade to PAN-OS 10.1.14-h8, PAN-OS 10.2.10-h12, PAN-OS 11.1.5, PAN-OS 11.2.3, or any newer versions released by Palo Alto Networks.

Workaround: As a temporary workaround for those unable to apply fixes immediately, disable DNS Security logging by navigating to Objects → Security Profiles → Anti-Spyware → DNS Policies, setting the "Log Severity" to "none" for all DNS Security categories, and committing the changes. Revert the settings after applying the necessary patches.

Restrict Network Access: Implement strict access controls to limit exposure of firewalls to untrusted networks. Only allow traffic from trusted sources to reach the firewall's data plane.

Continuous Monitoring: Implement continuous monitoring of firewall behavior to detect any unexpected reboots or instances of the system entering maintenance mode. Use centralized logging and alerting systems to promptly identify anomalies and investigate the root cause of such events.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0040 Impact	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1498 Network Denial of Service	T1529 System Shutdown/Reboot	T1190 Exploit Public-Facing Application

Patch Details

Update to the fixed versions of PAN-OS versions 10.1.14-h8, 10.2.10-h12, 11.1.5, 11.2.3, and all later versions. Prisma Access customers will receive updates in two phases during the weekends of January 3rd and January 10th, 2024.

Link: https://security.paloaltonetworks.com/CVE-2024-3393

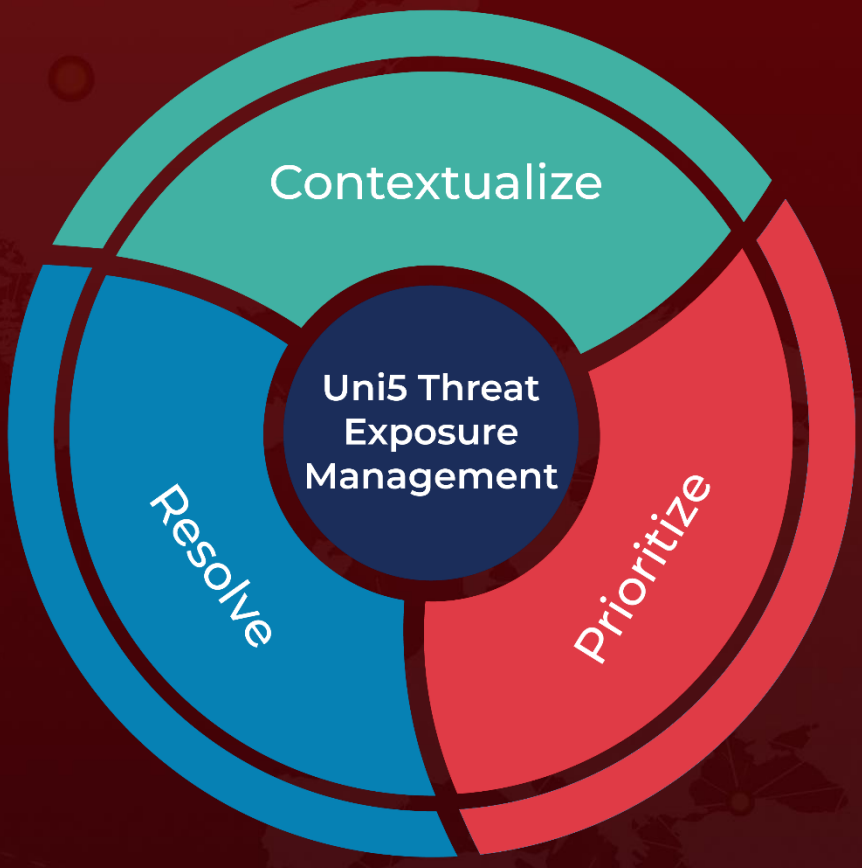
References

https://security.paloaltonetworks.com/CVE-2024-3393

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

December 27, 2024 • 5:45 AM

More at www.hivepro.com