KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | High-severity bug identified in Palo Alto's PAN-OS

Tracker ID: TN1016 **Date:** 13/Oct/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

On October 12th, Palo Alto issued a security advisory concerning a high-severity vulnerability impacting one of its PAN-OS products. The newly assigned CVE-2022-0030, is an authentication bypass vulnerability that affects Palo Alto Networks' PAN-OS 8.1. The vulnerability was discovered externally and impacts the web interface which could allow a network-based attacker with specific knowledge of the target firewall or Panorama appliance to perform privileged operations by impersonating an existing PAN-OS administrator.

The vulnerability affects PAN-OS versions before 8.1.24. However, to exploit this vulnerability the attacker must have network access to the PAN-OS web interface . PAN-OS 8.1 reached its software end-of-life (EoL) on March 1st, 2022, and is only supported on PA-200, PA-500, and PA-5000 Series firewalls, as well as M-100 appliances, until their respective hardware EoL dates. In addition, the EoL for the PA-5220's Next-Generation Firewall has been extended until December 31, 2022.

PAN-OS 8.1.24 and all subsequent PAN-OS versions have been patched to address the detected vulnerability. Customers with a Threat Prevention subscription can use Threat ID 92720 to prevent known attacks for this vulnerability (Applications and Threats content update 8630-7638). There have been no indications of malicious exploitation efforts for this bug. However, given the severity of the issue, it is recommended to apply the patches as soon as possible.

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-0030	High	8.1

Affected Products and Versions

- Vulnerable OS: PAN-OS 8.1 version < 8.1.24.
- Impacted Products: PA-200, PA-500 and PA-5000 Series next-generation firewalls and M-100 Panorama.

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | High-severity bug identified in Palo Alto's PAN-OS

Tracker ID: TN1016 **Date:** 13/Oct/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Recommendations

- Update to PAN-OS 8.1.24 or later PAN-OS versions.
- Follow RBAC and enable management access only for the people and services that must have access to manage the device.
- Inspect all traffic destined for the management port. Apply Security policy rules that specify the IP addresses of administrators and devices allowed access along with the applications, the source and destination zones allowed, and the authorized users.
- Monitor the services and critical assets exposed to the Internet. Collect and review relevant logs, data, and artifacts to identify any threat in the network.

References

- Palo Alto Networks Security Advisories, CVE-2022-0030 PAN-OS: Authentication Bypass in Web Interface, Reference PAN-195571, 12th October 2022, External Link (security.paloaltonetworks.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia