Advisory Alert

Alert Number: AAA20220512 **Date:** May 12, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Paloalto	High	Multiple Vulnerabilities

Description

Affected Product	**Paloalto**
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0024, CVE-2022-0025, CVE-2022-0026, CVE-2022-0027)
Description	Paloalto has released security patch updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2022-0024** - When the configuration is committed on both hardware and virtual firewalls, a vulnerability in Palo Alto Networks PAN-OS software allows an authenticated network-based PAN-OS administrator to upload a specially created configuration that disrupts system processes and potentially executes arbitrary code with root privileges. **CVE-2022-0025, CVE-2022-0026**- In Palo Alto Networks Cortex XDR agent software for Windows, a local privilege escalation (PE) vulnerability exists which allows an authorized local user with file creation privilege in the Windows root directory (such as C:) to execute a program with elevated privileges. **CVE-2022-0027**- Authenticated users in non-Read-Only groups can generate an email report that contains summary information about all incidents in the Cortex XSOAR instance, including incidents to which the user does not have access, due to an improper authorization vulnerability in Palo Alto Network Cortex XSOAR software.
Affected Products	PAN-OS 9.0 versions earlier than PAN-OS 9.0.16 PAN-OS 9.1 versions earlier than PAN-OS 9.1.13 PAN-OS 10.0 versions earlier than PAN-OS 10.0.10 PAN-OS 10.1 versions earlier than PAN-OS 10.1.5 Cortex XDR Agent 7.7.1.62043 without CU-500 on Windows Cortex XDR Agent 7.5.* without CU-330 on Windows Cortex XDR Agent 7.7.* without CU-330 on Windows Cortex XDR Agent 7.6.* without CU-330 on Windows Cortex XDR Agent 7.5.* without CU-330 on Windows Cortex XDR Agent 7.4.* without CU-330 on Windows Cortex XDR Agent 6.1.* without CU-330 on Windows Cortex XSOAR 6.1 Cortex XSOAR 6.2 Cortex XSOAR 6.5 Cortex XSOAR 6.6 versions earlier than Cortex XSOAR 6.6.0.2585049
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0024 https://security.paloaltonetworks.com/CVE-2022-0025 https://security.paloaltonetworks.com/CVE-2022-0026 https://security.paloaltonetworks.com/CVE-2022-0027

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.