Advisory Alert

Alert Number: AAA20201210 **Date:** December 10, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**High**	Multiple Vulnerabilities

Description

Affected Product	Palo Alto
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Palo Alto has released Security Updates which address multiple vulnerabilities across several of products, Palo alto highly recommends to apply relevant patches at earliest to avoid issues. **CVE-2020-2049** - A local privilege escalation vulnerability exists in Palo Alto Networks Cortex XDR Agent on the Windows platform that allows an authenticated local Windows user to execute programs with SYSTEM privileges. This requires the user to have the privilege to create files in the Windows root directory. **CVE-2020-2020** - An improper handling of exceptional conditions vulnerability in Cortex XDR Agent allows a local authenticated Windows user to create files in the software's internal program directory that prevents the Cortex XDR Agent from starting.
Affected Products	All versions of Cortex XDR Agent 7.1 with content update 149 and earlier versions; All versions of Cortex XDR Agent 7.2 with content update 149 and earlier versions. Cortex XDR Agent 5.0 versions earlier than 5.0.10; Cortex XDR Agent 6.1 versions earlier than 6.1.7; Cortex XDR Agent 7.0 versions earlier than 7.0.3; Cortex XDR Agent 7.1 versions earlier than 7.1.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2020-2049 https://security.paloaltonetworks.com/CVE-2020-2020

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.