Advisory Alert

Alert Number: AAA20220331 **Date:** March 31, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**High**	Denial-Of-Service (Dos) Vulnerability
VMware	**Medium**	Information Disclosure Vulnerability

Description

Affected Product	**Palo Alto**
Severity	**High**
Affected Vulnerability	Denial-Of-Service (Dos) Vulnerability (CVE-2022-0778)
Description	Paloalto has released Security Updates addressing an OpenSSL Infinite Loop Vulnerability that exists with Paloalto products. When parsing an invalid certificate, this vulnerability allows the OpenSSL library to enter an infinite loop, resulting in a Denial-of-Service (DoS) to the application. An attacker does not require a verified certificate to take advantage of this flaw since parsing a bad certificate triggers the infinite loop before the verification process is completed.
Affected Products	PAN-OS 8.1 versions earlier than PAN-OS 8.1.23 PAN-OS 9.0 versions earlier than PAN-OS 9.0.16-hf PAN-OS 9.1 versions earlier than PAN-OS 9.1.13-hf PAN-OS 10.0 versions earlier than PAN-OS 10.0.10 PAN-OS 10.1 versions earlier than PAN-OS 10.1.5-hf PAN-OS 10.2 versions earlier than PAN-OS 10.2.1 GlobalProtect app Cortex XDR agent
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0778

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2022-22948)
Description	VMware has released Security Update addressing Information Disclosure Vulnerability that exists with VMware products. An authenticated, local attacker with non-administrative (low-privileged user) access to the vulnerable vCenter Server instance could exploit this vulnerability to obtain sensitive information from the server. All VMware users are encouraged to upgrade to the latest versions.
Affected Products	VMware vCenter Server (vCenter Server) VMware Cloud Foundation (Cloud Foundation)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0009.html

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.