TLP: WHITE

Advisory Alert

Alert Number : AAA20201112 **Date :** November 12, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-27670, CVE-2020-27671, CVE-2020-27672, CVE-2020-27673, CVE-2020-27674, CVE-2020-27675)
Description	Citrix recently released security patch updates addressing multiple vulnerabilities that exists in their products. The most severe leads to unprivileged code in a PV guest VM to compromise that PV guest VM, privileged code in a guest VM to cause the host to crash or become unresponsive and privileged code in an HVM guest VM, to which the host administrator has assigned a PCI passthrough device, to corrupt in-memory data of the host or other VMs and potentially cause the host to crash. Citrix recommends that affected customers install these hotfixes at earliest to avoid facing issues.
Affected Products	Citrix Hypervisor Xen Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX284874

Affected Product	Palo Alto
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-1999, CVE-2020-2000, CVE-2020-2022, CVE-2020-2048, CVE-2020-2050)
Description	Palo Alto recently released security patch updates addressing multiple vulnerabilities including authentication bypass, sensitive information exposure, OS command injection and memory corruption that exists in their products with Pan-OS. It is highly recommended to apply necessary fixes at earliest to avoid facing issues.
Affected Products	All versions of PAN-OS 7.1 and PAN-OS 8.0. PAN-OS 8.1 versions earlier than PAN-OS 8.1.17 PAN-OS 9.0 versions earlier than PAN-OS 9.0.11 PAN-OS 9.1 versions earlier than PAN-OS 9.1.5 PAN-OS 10.0 versions earlier than PAN-OS 10.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://securityadvisories.paloaltonetworks.com/CVE-2020-1999 https://securityadvisories.paloaltonetworks.com/CVE-2020-2000 https://securityadvisories.paloaltonetworks.com/CVE-2020-2022 https://securityadvisories.paloaltonetworks.com/CVE-2020-2048 https://securityadvisories.paloaltonetworks.com/CVE-2020-2050

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.