Advisory Alert

Alert Number : AAA20200626 **Date :** June 26, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Citrix	**High**	Privilege Escalation
Vmware	**High**	Multiple Vulnerabilities
Cisco	**High**	Arbitrary Code Execution

Description

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Privilege Escalation (CVE-2020-13884, CVE-2020-13885)
Description	Due to insecure permissions and an unquoted path for %PROGRAMDATA%\Citrix in Citrix Workspace/Receiver, remote attacker could perform an exploit by copying a malicious citrix.exe and webio.dll to the affected systems and gain privileges during the uninstallation of the application on the targeted system.
Affected Products	Citrix Workspace App Citrix Receiver for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX275460

Affected Product	Vmware
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3962, CVE-2020-3963, CVE-2020-3964, CVE-2020-3965, CVE-2020-3966, CVE-2020-3967, CVE-2020-3968, CVE-2020-3969, CVE-2020-3970, CVE-2020-3971)
Description	VMware has released security updates to address multiple vulnerabilities that allows a malicious actor to access virtual machine locally. And a successful exploitation will allow the attacker to execute code on the hypervisor from a virtual machine.
Affected Products	VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) VMware Cloud Foundation
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0015.html

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution (CVE-2020-10188)
Description	Devices with Cisco IOS XE software that are configured with persistent Telnet feature is vulnerable. A remote attackers can execute arbitrary codes via short writes or urgent data involving the netclear and nextitem functions.
Affected Products	Cisco IOS XE Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-telnetd-EFJrEzPx

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.