Advisory Alert

Alert Number: AAA20201121 **Date:** November 21, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple vulnerabilities
Cisco	**Critical**	CVE-2020-27130 : Path Traversal (AAA20201117)

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-4004 ,CVE-2020-4005)
Description	VMware has released security updates addressing the critical Multiple vulnerability in VMware products. **CVE-2020-4004 -** VMware ESXi, Workstation contains a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. **CVE-2020-4005 -** VMware ESXi contains a privilege-escalation vulnerability that exists in the way certain system calls are being managed. A malicious actor with privileges within the process only may escalate their privileges. Successful exploitation of this issue is only possible when chained with another vulnerability
Affected Products	VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0026.html

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Path Traversal (CVE-2020-27130)
Description	The vulnerability could allow an unauthenticated, remote attacker to gain access to and modify sensitive information on the affected device. Improper validation of directory traversal character sequences within requests to an affected device. An attacker could exploit and send a crafted request to allow the attacker to read or write arbitrary files on the affected device.
Affected Products	Cisco Security Manager releases 4.21 and earlier.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csm-path-trav-NgeRnqgR

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.