Advisory Alert

Alert Number : AAA20200603 **Date :** June 3, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	IP Packet Processing Vulnerability
VMware	**High**	Denial-of-service Vulnerability

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	IP Packet Processing Vulnerability (CVE-2020-10136)
Description	Cisco NX-OS Software network stack contains a vulnerability seem permit an attacker who is unauthenticated to go through certain security measures. The cause of this vulnerability is due to the fact that affected device decapping and processing the IP contain in the IP packets accidentally as those packets are destined to a locally configured IP address. Furthermore, Beneath certain conditions, a successful exploit might cause the network stack process to crash and restart couple of times, driving to a reload of the influenced system and a DoS condition.
Affected Products	Nexus 1000 Virtual Edge for VMware vSphere (CSCvu10050) Nexus 1000V Switch for Microsoft Hyper-V (CSCvt67738) Nexus 1000V Switch for VMware vSphere (CSCvt67738) Nexus 3000 Series Switches (CSCun53663) Nexus 5500 Platform Switches (CSCvt67739) Nexus 5600 Platform Switches (CSCvt67739) Nexus 6000 Series Switches (CSCvt67739) Nexus 7000 Series Switches (CSCvt66624) Nexus 9000 Series Switches in standalone NX-OS mode (CSCun53663) UCS 6200 Series Fabric Interconnects (CSCvu03158) UCS 6300 Series Fabric Interconnects (CSCvt67740)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ipip-dos-kCT9X4

Affected Product	VMware
Severity	**High**
Affected Vulnerability	Denial-Of-Service Vulnerability (CVE-2020-3958)
Description	A denial-of-service vulnerability has been discovered in the “shader functionality” of multiple vmware products. In order this exploit to be successful, the attacker should have access to a 3D graphics enabled virtual machine and if the attempt is successful, this could allow attackers with non-administrative access to a virtual machine to crash the virtual machine's vmx process driving to a denial of service condition.
Affected Products	ESXi 7.0, ESXi 6.7, ESXi 6.5, Workstation 15.x, Fusion 11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0011.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.