TLP: WHITE

Advisory Alert

Alert Number: AAA20201105 **Date:** November 5, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	CVE-2020-3992 : Remote code execution.(AAA20201021)
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical -** Initial release date is 20th Oct 2020. This patch is again sent as a reminder to update since the earlier patch did not address the CVE-2020-3992 completely.
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3981, CVE-2020-3982, CVE-2020-3992, CVE-2020-3993, CVE2020-3994, CVE-2020-3995)
Description	OpenSLP as utilized in ESXi, features a use-after-free issue (Use After Free specifically refers to the attempt to access memory after it has been freed, which can cause a program to crash or, in the case of a Use-After-Free flaw, can potentially result in the execution of arbitrary code or even enable full remote code execution capabilities.). A malicious actor residing within the management network who has access to port 427 on an ESXi machine could also trigger a use-after-free within the OpenSLP service leading to remote code execution. The ESXi patches released on October 20, 2020, didn't address CVE-2020-3992 completely. Therefore, it is better to check the latest patch available and apply according to the link provided in the advisory.
Affected Products	VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro Fusion (Fusion) NSX-T VMware vCenter Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0023.html

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3284 , CVE-2020-26071 , CVE-2020-26074 , CVE-2020-26073 , CVE-2020-3594 , CVE-2020-3600 , CVE-2020-3593 , CVE-2020-3595 , CVE-2020-3579 , CVE-2020-3591 , CVE-2020-3587 , CVE-2020-3590 , CVE-2020-26066 , CVE-2020-26064 , CVE-2020-3592 , CVE-2020-26065 , CVE-2020-27129 , CVE-2020-27128 , CVE-2020-3444)
Description	Cisco has released updates addressing multiple vulnerabilities that exists in Cisco SD-WAN and Cisco IOS XR Software. It is highly recommended to apply necessary fixes provided in official Cisco website at earliest to avoid these vulnerabilities.
Affected Products	SD-WAN vBond Orchestrator Software SD-WAN vEdge Cloud Routers SD-WAN vEdge Routers SD-WAN vManage Software SD-WAN vSmart Controller Software Cisco IOS XR Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x

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.