TLP: WHITE

Advisory Alert

Alert Number: AAA20201021 **Date:** October 21, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**High**	Multiple Vulnerabilities
Oracle	**High**	Multiple Vulnerabilities
Cisco	**High**	Arbitrary Code Execution

Description

Affected Product	VMware
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3981, CVE-2020-3982, CVE-2020-3992, CVE-2020-3993, CVE-2020-3994, CVE-2020-3995)
Description	VMware products have multiple vulnerabilities in which a remote attacker could exploit to trigger a remote code execution, NSX-T MITM , out-of-bounds, session hijack, memory leak on the targeted system.
Affected Products	VMware ESXi VMware Workstation Pro / Player (Workstation) VMware Fusion Pro / Fusion (Fusion) NSX-T
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0023.html

Affected Product	Oracle
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released its October 2020 Critical patch update containing a collection of patches to address several security vulnerabilities affected by multiple products.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuoct2020.html

Affected Product	Cisco
Severity	**High -** Initial release date 05 Feb 2020 it is again added as a reminder the update is sent as there is attempted exploitation of this vulnerability in the wild
Affected Vulnerability	Arbitrary Code Execution (CVE-2020-3118)
Description	A vulnerability in the Cisco Discovery Protocol could allow an unauthenticated, attacker to execute arbitrary code or cause a reload on an affected device. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device successful exploit could allow the attacker to cause a stack overflow, which could allow the attacker to execute arbitrary code with administrative privileges on an affected device. Cisco recommends that customers upgrade to a fixed Cisco IOS XR Software release.
Affected Products	ASR 9000 Series Aggregation Services Routers Carrier Routing System (CRS) IOS XRv 9000 Router Network Convergence System (NCS) 540 Series Routers Network Convergence System (NCS) 560 Series Routers Network Convergence System (NCS) 1000 Series Routers Network Convergence System (NCS) 5000 Series Routers Network Convergence System (NCS) 5500 Series Routers Network Convergence System (NCS) 6000 Series Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200205-iosxr-cdp-rce

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.