Advisory Alert

Alert Number : AAA20210224 **Date :** February 24, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Arbitrary File Read Vulnerability

Description

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-21972, CVE-2021-21973, CVE-2021-21974)
Description	VMware has fixed critical vulnerabilities including remote code execution, heap overflow, SSRF vulnerability. CVE-2021-21972: The vSphere Client contains a remote code execution vulnerability in a vCenter Server plugin. A remote non authenticated attacker can send a specially crafted HTTP request to port 443 and execute arbitrary code on the system. CVE-2021-21973: The disclosed vulnerability allows a remote attacker to perform SSRF attacks.An Attacker with network access to port 443 may exploit this issue by sending a POST request to vCenter Server plugin leading to information disclosure. CVE-2021-21974: OpenSLP as used in ESXi has a heap-overflow vulnerability. A remote non authenticated attacker on the local network can send specially crafted packets to port 427 trigger a heap based buffer overflow and execute arbitrary code on the target system.
Affected Products	VMware ESXi VMware vCenter Server (vCenter Server) VMware Cloud Foundation (Cloud Foundation)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0002.html

Affected Product	RedHat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-14351, CVE-2020-24394, CVE-2020-25212, CVE-2020-25705, CVE-2020-29661)
Description	Multiple vulnerabilities were identified in Linux Kernel, a remote attacker could exploit some of these vulnerabilities to trigger elevation of privilege, remote code execution and sensitive information disclosure on the targeted system. Redhat Highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:0526 https://access.redhat.com/errata/RHSA-2021:0537 https://access.redhat.com/errata/RHSA-2021:0558

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Arbitrary File Read Vulnerability (CVE-2021-1258)
Description	A vulnerability in the upgrade component of Cisco AnyConnect Secure Mobility Client could allow an authenticated, local attacker with low privileges to read arbitrary files on the underlying operating system of an affected device. An attacker could exploit this vulnerability by sending a crafted command from the local CLI to the application.
Affected Products	AnyConnect Secure Mobility Client for Linux, MacOS and Windows releases earlier than Release 4.9.03047.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-fileread-PbHbgHMj

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.