Advisory Alert

Alert Number: AAA20210331 **Date:** March 31, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	**Multiple Vulnerabilities**
Citrix	**High**	Multiple vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	VMware
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-21975, CVE-2021-21983)
Description	VMware has released security patch updates addressing multiple vulnerabilities that exists in their products. CVE-2021-21975 - An attacker with network access to the vRealize Operations Manager can exploit this vulnerability and perform a server side request forgery attack to steal administrative credentials CVE-2021-21983 - Using this flaw an authenticated attacker with network access to the vRealize Operations Manager has the ability to write files to arbitrary location on the underlying photon OS.
Affected Products	VMware vRealize Operations VMware Cloud Foundation vRealize Suite Lifecycle Manager
Officially Acknowledged by the Vendor	yes
Patch/ Workaround Released	yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0004.html

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-28688, CVE-2021-28038, CVE-2020-35498)
Description	Citrix released security patch updates addressing multiple vulnerabilities that exists in their products CVE-2021-28688, CVE-2021-28038 - An attacker with ability to execute privileged mode codes in a guest and cause denial of service attack against the host. CVE-2020-35498 - This flaw allows malicious network traffic on local network to cause subsequent packets to be dropped
Affected Products	Citrix Hypervisor versions up to Citrix Hypervisor 8.2 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX306565

Affected Product	Redhat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-17563,CVE-2020-1935,CVE-2019-5482,CVE-2020-29661)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exists with multiple Redhat products. The most severe could cause use-after-free vulnerability and Redhat highly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 7.7 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 7.7 s390x Red Hat Enterprise Linux for Power, big endian - Extended Update Support 7.7 ppc64 Red Hat Enterprise Linux EUS Compute Node 7.7 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 7.7 ppc64le Red Hat Enterprise Linux Server - TUS 7.7 x86_64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 7.7 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2019-17563 https://access.redhat.com/security/cve/CVE-2020-1935 https://access.redhat.com/security/cve/CVE-2019-5482 https://access.redhat.com/security/cve/CVE-2020-29661

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1385, CVE-2021-1224)
Description	CVE-2021-1385 - Due to improper validation of URIs in IOx API requests an attacker could exploit an affected device by sending crafted API requests that contains directory traversal character sequence. Successful exploitation could allow the attacker to read/write arbitrary files on underlying OS. CVE-2021-1224 - An attacker could send crafted TFO packets with an HTTP payload through an affected device and the success exploitation of this vulnerability could allow an unauthenticated attacker to bypass a configured file policy for HTTP packets and deliver a malicious payload.
Affected Products	3000 Series Industrial Security Appliances (ISAs) Firepower Threat Defense (FTD) Software Meraki MX64 Meraki MX64W Meraki MX67 Meraki MX67C Meraki MX67W Meraki MX68 Meraki MX68CW Meraki MX68W Meraki MX84 Meraki MX100 Meraki MX250 Meraki MX450 1000 Series Integrated Services Routers (ISRs) 4000 Series ISRs Catalyst 8000V Edge Software Catalyst 8200 Series Edge Platforms Catalyst 8300 Series Edge Platforms Catalyst 8500L Edge Platforms Cloud Services Router 1000V (CSR 1000V) Integrated Services Virtual Router (ISRv) 809 Industrial Integrated Services Routers (ISRs) 829 Industrial ISRs CGR 1000 Compute Module IC3000 Industrial Compute Gateway Devices running Cisco IOS XE Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-tfo-bypass-MmzZrtes https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-pt-hWGcPf7g

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.