Advisory Alert

Alert Number: AAA20210304 **Date:** March 4, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	High	Multiple Vulnerabilities
Redhat	High	Multiple Vulnerabilities
VMware	High	Remote code execution vulnerability
Cpanel	High	Multiple Vulnerabilities
Cisco	High	Multiple Vulnerabilities
Joomla	Low	Multiple Vulnerabilities

Description

Affected Product	Fortinet
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-15938, CVE-2020-6648, CVE-2018-13380, CVE-2021-22128, CVE-2019-17655)
Description	Fortinet has released Security Updates addressing multiple vulnerabilities such as information disclosure, cross site scripting, improper access control, and traffic bypass that exists in FortiProxy and Fortigate products.
Affected Products	FortiProxy version 2.0.0 FortiProxy versions 1.2.9 and below. FortiProxy versions 1.1.6 and below. FortiProxy versions 1.0.7 and below. FortiProxy versions 1.2.8 and below. FortiGate versions 6.4.2 and below. FortiGate versions 6.2.5 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-20-224 https://www.fortiguard.com/psirt/FG-IR-20-235 https://www.fortiguard.com/psirt/FG-IR-20-230 https://www.fortiguard.com/psirt/FG-IR-20-236 https://www.fortiguard.com/psirt/FG-IR-20-172

Affected Product	Redhat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-14372, CVE-2020-14351, CVE-2020-14781, CVE-2020-14782, CVE-2020-14803, CVE-2020-25632, CVE-2020-25647, CVE-2020-25705, CVE-2020-0444, CVE-2021-20225, CVE-2021-20233, CVE-2020-27749, CVE-2020-27779, CVE-2020-2773,CVE-2020-27221, CVE-2020-29661, CVE-2020-35517)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exists with multiple Redhat products. Redhat highly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	Multiple Redhat Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2020-35517 https://access.redhat.com/security/cve/CVE-2020-0444 https://access.redhat.com/security/cve/CVE-2020-14351 https://access.redhat.com/security/cve/CVE-2020-25705 https://access.redhat.com/security/cve/CVE-2020-29661 https://access.redhat.com/security/cve/CVE-2020-2773 https://access.redhat.com/security/cve/CVE-2020-14781 https://access.redhat.com/security/cve/CVE-2020-14782 https://access.redhat.com/security/cve/CVE-2020-14803 https://access.redhat.com/security/cve/CVE-2020-27221 https://access.redhat.com/security/cve/CVE-2020-14372 https://access.redhat.com/security/cve/CVE-2020-25632 https://access.redhat.com/security/cve/CVE-2020-25647 https://access.redhat.com/security/cve/CVE-2020-27749 https://access.redhat.com/security/cve/CVE-2020-27779 https://access.redhat.com/security/cve/CVE-2021-20225 https://access.redhat.com/security/cve/CVE-2021-20233

Affected Product	VMware
Severity	High
Affected Vulnerability	Remote code execution vulnerability (CVE-2021-21978)
Description	Vmware view planner is vulnerable for remote code execution vulnerability due to Improper input validation and lack of authorization leading to arbitrary file upload in logupload web application. Using this flaw an unauthorized attacker with network access to View Planner Harness has the ability to upload and execute a specially crafted file causing remote code execution within the logupload container.
Affected Products	VMware View Planner
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0003.html

Affected Product	Cpanel
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-8265, CVE-2020-8287, CVE-2020-1971)
Description	Cpanel released security patches addressing multiple vulnerabilities that exists in the product. CVE-2020-8265 - Node.js is vulnerable to a use-after-free bug in its TLS implementation and successful exploitation could cause corrupt memory leading to a Denial of Service or potentially other exploits. CVE-2020-8287 - Flaw that exists in Node.js could allow two copies of a header field in an HTTP request. Due to that issue Node.js identifies the first header field and ignores the second and this can lead to HTTP Request Smuggling. CVE-2020-1971 - An attacker can trick a client or server into checking a malicious certificate against a malicious CRL using this flaw.
Affected Products	All versions of NodeJS through 10.23.3.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-4-march-3-release/

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1285 ,CVE-2021-1410 ,CVE-2021-1465 ,CVE-2021-1464 ,CVE-2021-1424 ,CVE-2021-1232 ,CVE-2021-1466 ,CVE-2021-1461 ,CVE-2021-1462 ,CVE-2021-1470 ,CVE-2021-1132 ,CVE-2020-3551 ,CVE-2020-26063)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exists with multiple Cisco products. Cisco highly recommends to apply necessary fixes to the products at earliest to avoid issues.
Affected Products	Multiple Cisco Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	**Cisco SD-WAN** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-sigverby-pass-gPYXd6Mk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vdae-mon-bo-RuzzEA2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-autho-rization-b-GUEpSLK https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vman-dir-trav-Bpwc5gtm https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanvman-in-fodis1-YuQScHB https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdw-sqlinj-HD-JUeEAX https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-vman-kth3c82B **Cisco ASR 5000 Series Software** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-staros-ipsecmgr-dos-3gkHXwvS **Cisco Email Security Appliance and Content Security Management Appliance** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-info-disclo-VOu2GHbZ **Cisco IP Phone Series 68xx/78xx/88xx** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-rce-dos-U2PsSkz3 **Cisco Network Services Orchestrator** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-path-trvsl-dZRQE8Lc **Cisco Webex Meetings** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-distupd-N87eB6Z3 **Cisco Products Snort Ethernet Frame Decoder** https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-ethernet-dos-HGXgJH8n

Affected Product	Joomla
Severity	**Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-23131,CVE-2021-23126, CVE-2021-23127,CVE-2021-23128,CVE-2021-23129,CVE-2021-26028,CVE-2021-23130,CVE-2021-23132, CVE-2021-26027,CVE-2021-26029)
Description	Joomla has released patch updates addressing multiple vulnerabilities that exists in their products. It is highly recommended by Joomla to apply necessary fixes at earliest to avoid issues.
Affected Products	Joomla! CMS versions 1.6.0 - 3.9.24 Joomla! CMS versions 3.0.0 - 3.9.24 Joomla! CMS versions 2.5.0 - 3.9.24 Joomla! CMS versions 3.2.0 - 3.9.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre.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.