Advisory Alert

Alert Number: AAA20210922 **Date:** September 22, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMWare	**Critical**	Multiple Vulnerabilities
Redhat	**Medium**	Multiple Vulnerabilities
Apache	**Medium**	Multiple Vulnerabilities

Description

Affected Product	VMWare
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-21991, CVE-2021-21992, CVE-2021-21993, CVE-2021-22005, CVE-2021-22006, CVE-2021-22007, CVE-2021-22008, CVE-2021-22009, CVE-2021-22010, CVE-2021-22011, CVE-2021-22012, CVE-2021-22013, CVE-2021-22014, CVE-2021-22015, CVE-2021-22016, CVE-2021-22017, CVE-2021-22018, CVE-2021-22019, CVE-2021-22020)
Description	VMWare has released security updates addressing multiple vulnerabilities that exists in their products including server side request forgery, denial-of-service, information disclosure, server file deletion, server file upload, authenticated code execution, rhttpproxy bypass, reflected XSS, file path traversal, unauthenticated API information disclosure, local privilege escalation, reverse proxy bypass, unauthenticated API endpoint. It is highly recommended by VMWare to apply necessary security fixes at earliest to avoid issues.
Affected Products	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-2021-0020.html

Affected Product	Redhat
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. This includes security update for curl packages, security/bug fix/enhancement updates for mysql:8.0 and security/bug fix update for nodejs:12. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.4 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.4 x86_64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP So Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:3590 https://access.redhat.com/errata/RHSA-2021:3582 https://access.redhat.com/errata/RHSA-2021:3623

Affected Product	Apache
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33193, CVE-2021-34798, CVE-2021-36160, CVE-2021-39275, CVE-2021-40438)
Description	Apache has released security updates addressing multiple vulnerabilities that exists in their products including request splitting via HTTP/2 method injection and mod_proxy, NULL pointer dereference in httpd core, mod_proxy_uwsgi out of bound read, ap_escape_quotes buffer overflow and mod_proxy server side request forgery. Apache highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Prior to update 2.4.49
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.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.