Advisory Alert

Alert Number: AAA20210407 **Date:** April 7, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	High	Multiple Vulnerabilities
Fortinet	Medium	Multiple Vulnerabilities

Description

Affected Product	Redhat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-35518,CVE-2021-20277,CVE-2020-0466,CVE-2020-27152,CVE-2020-28374,CVE-2021-3347, CVE-2021-26708,CVE-2021-27363,CVE-2021-27364,CVE-2021-27365)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exists with multiple Redhat products. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Gluster Storage Server for On-premise 3 for RHEL 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Virtualization Host 4 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2020-35518 https://access.redhat.com/security/cve/CVE-2021-20277 https://access.redhat.com/security/cve/CVE-2020-0466 https://access.redhat.com/security/cve/CVE-2020-27152 https://access.redhat.com/security/cve/CVE-2020-28374 https://access.redhat.com/security/cve/CVE-2021-3347 https://access.redhat.com/security/cve/CVE-2021-26708 https://access.redhat.com/security/cve/CVE-2021-27363 https://access.redhat.com/security/cve/CVE-2021-27364 https://access.redhat.com/security/cve/CVE-2021-27365

Affected Product	Fortinet
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-17656,CVE-2020-15942,CVE-2018-13380,CVE-2021-24024)
Description	Fortinet has released security updates addressing multiple vulnerabilities such as buffer overflow, information disclosure, cross-site scripting. It is highly recommended by Fortinet to apply necessary security fixes at earliest to avoid issues.
Affected Products	FortiProxy versions 2.0.1, 1.2.9 and below FortiProxy versions 1.1.x. FortiProxy versions 1.0.x. FortiWeb version 6.2.3,6.3.4 and below. FortiProxy version 2.0.0 FortiProxy versions 1.2.8, 1.1.6, 1.0.7 and below. FortiADCManager versions 5.2.1, 5.3.0 and below. FortiADC versions 5.3.7 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-21-007 https://www.fortiguard.com/psirt/FG-IR-20-076 https://www.fortiguard.com/psirt/FG-IR-20-230 https://www.fortiguard.com/psirt/FG-IR-19-244

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.