Advisory Alert

Alert Number: AAA20210908 **Date:** September 8, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortigate	High	Multiple Vulnerabilities
Redhat	Medium	Multiple Vulnerabilities

Description

Affected Product	Fortigate	
Severity	High	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22127, CVE-2021-26116, CVE-2021-36179, CVE-2021-36182, CVE-2020-29012, CVE-2020-29013, CVE-2021-32600, CVE-2021-36169, CVE-2021-24017, CVE-2021-24016)	
Description	Fortigate has released security updates addressing multiple vulnerabilities that exists in their products including arbitrary code execution, improper authentication, information disclosure and denial of service. It is highly recommended by Fortigate to apply necessary security fixes at earliest to avoid issues.	
Affected Products	FortiOS 7.0.0 FortiOS 6.4.6 and below FortiOS 6.2.x FortiOS 6.0.x FortiOS 5.6.x FortiSandbox 3.2.1 and below. FortiSandbox 3.1.4 and below. FortiManager 6.2.6 and below. FortiManager v6.4.3 and below. FortiManager v6.2.7 and below. FortiAuthenticator 6.3.0 and below. FortiAuthenticator 6.2.1 and below.	FortiAuthenticator 6.2.0 and below FortiWeb version 6.3.13 or below is impacted FortiWeb version 6.2.4 or below is impacted FortiWeb version 6.3.14 or below FortiWeb version 6.2.4 or below Any FortiGate version 7.0.0 or below is impacted. Any FortiGate version 6.4.6 or below is impacted. Any FortiGate version 6.2.9 or below is impacted. FortiSandbox versions 3.2.1 and below. FortiClient for Linux versions 6.2.8 and below. FortiClient for Linux versions 6.4.2 and below.
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-20-241 https://www.fortiguard.com/psirt/FG-IR-21-068 https://www.fortiguard.com/psirt/FG-IR-20-206 https://www.fortiguard.com/psirt/FG-IR-21-047 https://www.fortiguard.com/psirt/FG-IR-20-070 https://www.fortiguard.com/psirt/FG-IR-20-178 https://www.fortiguard.com/psirt/FG-IR-20-243 https://www.fortiguard.com/psirt/FG-IR-21-091 https://www.fortiguard.com/psirt/FG-IR-20-189 https://www.fortiguard.com/psirt/FG-IR-20-190	

Affected Product	Redhat	
Severity	Medium	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-38201, CVE-2021-3609, CVE-2021-3715, CVE-2021-37576)	
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could result in OS memory corruption and local privilege escalation. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.	
Affected Products	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 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 Enterprise Linux for Power, little endian 7 ppc64le Red Hat Virtualization Host 4 for RHEL 7 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.1 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.1 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.1 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.1 aarch64	Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.1 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.1 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.1 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.1 aarch64 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 Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://access.redhat.com/errata/RHSA-2021:3438 https://access.redhat.com/errata/RHSA-2021:3444 https://access.redhat.com/errata/RHSA-2021:3440	

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.