Advisory Alert

Alert Number: AAA20220608 **Date:** June 8, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortigate	**Critical**	Multiple Vulnerabilities
Fortigate	**High**, **Medium**	Multiple Vulnerabilities
Redhat	**Medium**	Memory Disclosure

Description

Affected Product	Fortigate
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-13927, CVE-2020-11982, CVE-2020-11981, CVE-2021-35936, CVE-2021-28359, CVE-2020-17526, CVE-2020-17513)
Description	Fortigate has released security updates addressing multiple critical vulnerability that exists in FortiAnalyzer product which contains a vulnerable version of apache airflow library. Fortigate recommends upgrade their mentioned versions to avoid these issues.
Affected Products	FortiAnalyzer version 7.0.2 and below. FortiAnalyzer version 6.4.7 and below.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-22-008

Affected Product	Fortigate	
Severity	**High**, **Medium**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-30301, CVE-2022-22304, CVE-2022-26113, CVE-2022-29060, CVE-2021-22131, CVE-2022-22305)	
Description	Fortigate has released security updates addressing multiple vulnerabilities that exists in their products including unauthorized code or commands execution, Information disclosure, Improper access control, Improper server authentication. Fortigate recommends to apply necessary security fixes at earliest to avoid issues.	
Affected Products	FortiAP-U version 6.2.0 through 6.2.3 FortiAP-U version 6.0.0 through 6.0.4 FortiAP-U version 5.4.0 through 5.4.6 FortiAuthenticator Agent for Microsoft OWA version 2.2, FortiAuthenticator Agent for Microsoft OWA version 2.1 FortiClientWindows version 6.0.0 through 6.0.10 FortiClientWindows version 6.2.0 through 6.2.9 FortiClientWindows version 6.4.0 through 6.4.7 FortiClientWindows version 7.0.0 through 7.0.3 FortiDDoS version 5.5.0 through 5.5.1 FortiDDoS version 5.4.0 through 5.4.2 FortiDDoS version 5.3.0 through 5.3.1 FortiDDoS version 5.2.0 FortiDDoS version 5.1.0	FortiTokenMobile for Android v5.0.3 or below is impacted FortiTokenMobile for iOS v5.2.0 or below is impacted FortiTokenMobile for Windows v4.0.3 or below is impacted FortiOS versions 6.2.x FortiOS versions 6.0.x FortiManager version 7.0.1 and below. FortiManager version 6.4.6 and below. FortiAnalyzer version 7.0.2 and below. FortiAnalyzer version 6.4.7 and below. FortiSandbox versions 4.0.x. FortiSandbox versions 3.2.x. FortiSandbox versions 3.1.5 and below.
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-22-109 https://www.fortiguard.com/psirt/FG-IR-22-021 https://www.fortiguard.com/psirt/FG-IR-22-044 https://www.fortiguard.com/psirt/FG-IR-22-071 https://www.fortiguard.com/psirt/FG-IR-21-024 https://www.fortiguard.com/psirt/FG-IR-18-292	

Affected Product	Redhat
Severity	**Medium**
Affected Vulnerability	Memory Disclosure (CVE-2021-3677)
Description	Redhat has released security updates addressing memory disclosure vulnerability that exists in their Red Hat Virtualization products. A flaw which exist in Postgresql allows a specially crafted query to read arbitrary bytes of server memory. By default, any authenticated database user can carry out this attack at any time. The ability to create objects is not required for the attack. The known versions of this attack are infeasible if server settings include max worker processes=0.Also there may be attacks due to undiscovered variant which are independent from that setting
Affected Products	Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:4931

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.