Advisory Alert

Alert Number: AAA20220406 **Date:** April 6, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortinet	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities

Description

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-44167, CVE-2021-43205, CVE-2021-44169, CVE-2022-23446, CVE-2022-23440, CVE-2022-23441, CVE-2021-32593, CVE-2021-24009, CVE-2021-26114, CVE-2021-26112, CVE-2021-32585, CVE-2021-26113, CVE-2021-26093)
Description	Fortinet has released Security Updates addressing multiple vulnerabilities that exist with Fortinet products. All Fortinet users are encouraged to upgrade to the latest versions of your Fortinet products. • CVE-2021-44167: FortiClient (Linux) - Improper directories permissions • CVE-2021-43205: FortiClient (Linux) - external access to confighandler webserver • CVE-2021-44169: FortiClient (Windows) - privilege escalation in online installer due to incorrect working directory • CVE-2022-23446: FortiEDR - Denial of service due to folder access permission change • CVE-2022-23440: FortiEDR - Hardcoded AES key enable disabling local Collector • CVE-2022-23441: FortiEDR - Insecure RSA key transport • CVE-2021-32593: FortiWAN - Improper cryptographic operations in Dynamic Tunnel Protocol • CVE-2021-24009: FortiWAN - Pervasive OS command injection • CVE-2021-26114: FortiWAN - Pervasive SQL injection • CVE-2021-26112: FortiWAN - Stack-based buffer overflow in bmstatd • CVE-2021-32585: FortiWAN - Stored Cross-site scripting in log viewer • CVE-2021-26113: FortiWAN - Use of hardcoded salt for password hashing • CVE-2021-26093: FortiWLC - Access of Uninitialized Pointer vulnerability
Affected Products	FortiClient Linux Multiple Versions FortiClient for Linux Multiple Versions FortiClient (Windows) Multiple Versions FortiEDR Collector version 5.0.3 b0233 and earlier FortiEDR version 4.0.0 FortiEDR version 5.0.0 through 5.0.2 FortiWAN 4.5.8 and earlier FortiWAN 4.5.8 and below FortiWAN version 4.5.8 and below FortiWLC Multiple Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt?date=04-2022

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0435, CVE-2021-4028, CVE-2021-4083)
Description	Red Hat has released Security Updates addressing multiple kernel vulnerabilities that exist with Red Hat products. These vulnerabilities allow for Code Execution, Denial-of-Service (DoS), and Privilege Escalation or crash the system, all Red Hat users are encouraged to upgrade to the latest versions.
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:1185 https://access.redhat.com/errata/RHSA-2022:1186

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.