Advisory Alert

Alert Number: **AAA20250825** **Date:** **August 25, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**	Denial of Service Vulnerability
F5	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NetApp	**Medium**	Security Update

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22058, CVE-2025-37914, CVE-2025-38417, CVE-2022-50020, CVE-2025-21919, CVE-2025-22020, CVE-2025-38086, CVE-2025-38380, CVE-2025-38000, CVE-2025-38177, CVE-2025-38350)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server - AUS 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:14420 • https://access.redhat.com/errata/RHSA-2025:14418 • https://access.redhat.com/errata/RHSA-2025:14413

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-48976)
Description	IBM has released a security update addressing a denial-of-service vulnerability that exists in their product. **CVE-2025-48976** - Allocation of resources for multipart headers with insufficient limits enabled a DoS vulnerability in Apache Commons FileUpload. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server - 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7242915

Affected Product	**F5**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-0086, CVE-2021-0089, CVE-2025-49794, CVE-2025-49795, CVE-2025-49796, CVE-2019-11599, CVE-2016-1762, CVE-2016-1840, CVE-2016-1834, CVE-2024-8176, CVE-2016-4447, CVE-2016-4449)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to information disclosure, Unauthorized modifications, denial of service attacks. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K41043270 • https://my.f5.com/manage/s/article/K000153130 • https://my.f5.com/manage/s/article/K51674118 • https://my.f5.com/manage/s/article/K14338030 • https://my.f5.com/manage/s/article/K14614344 • https://my.f5.com/manage/s/article/K16712298 • https://my.f5.com/manage/s/article/K000151869 • https://my.f5.com/manage/s/article/K24322529

Affected Product	**NetApp**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2024-10978)
Description	NetApp has released a security update addressing a vulnerability that exists in brocade SAN navigator. **CVE-2024-10978** - Multiple NetApp products incorporate Postgresql. Certain versions of PostgreSQL are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Brocade SAN Navigator (SANnav)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250822-0003

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.