Advisory Alert

Alert Number: AAA20240820 **Date:** August 20, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
NetApp	**High**	Linux Kernel Vulnerability
F5	**High**	BIND vulnerability
HPE	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36971, CVE-2024-36886)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-36971** - A use-after-free flaw was found in the Linux kernel's network route management. This flaw allows an attacker to alter the behavior of certain network connections. **CVE-2024-36886** - A use-after-free (UAF) flaw exists in the Linux Kernel within the reassembly of fragmented TIPC messages, specifically in the tipc_buf_append() function. The issue results due to a lack of checks in the error handling cleanup and can trigger a UAF on "struct sk_buff", which may lead to remote code execution. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64, x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64, AUS 9.4 x86_64, TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:5519 • https://access.redhat.com/errata/RHSA-2024:5520 • https://access.redhat.com/errata/RHSA-2024:5521 • https://access.redhat.com/errata/RHSA-2024:5522 • https://access.redhat.com/errata/RHSA-2024:5523

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Linux Kernel Vulnerability (CVE-2023-52340)
Description	NetApp has release security update addressing a Linux Kernel Vulnerability that exists in their products. **CVE-2023-52340** - Linux kernel versions prior to 6.3-rc1 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	E-Series SANtricity OS Controller Software 11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20240816-0005/

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	BIND vulnerability (CVE-2024-1737)
Description	F5 has release security updates addressing a BIND vulnerability that affects F5 products. A remote attacker can trigger excessive resource consumption on the vulnerable system to cause a denial-of-service (DoS). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (DNS) – Versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000140732

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20578, CVE-2021-26344, CVE-2023-20591, CVE-2023-20584, CVE-2021-46746, CVE-2023-31356, CVE-2021-26387, CVE-2021-46772, CVE-2023-20518)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Arbitrary Code Execution, Denial of Service, Disclosure of Privileged Information, Buffer Overflow. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE SimpliVity 325 Gen 11 - Prior to HPE SimpliVity Support Pack (SVTSP) version SVTSPGen11-2024_0731 • HPE SimpliVity 325 Gen10 - Prior to HPE SimpliVity Support Pack (SVTSP) version SVTSPGen10-2024_0731 • HPE SimpliVity 325 Gen10 Plus - Prior to HPE SimpliVity Support Pack (SVTSP) version SVTSPGen10-2024_0731
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04687en_us&docLocale=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Out of Bounds Read, Memory Leakage, Use After Conditions, NULL-pointer dereferences. SUSE 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://www.suse.com/support/update/announcement/2024/suse-su-20242939-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242940-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242943-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242944-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242947-1 • https://www.suse.com/support/update/announcement/2024/suse-su-20242948-1

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-50315, CVE-2020-8908, CVE-2023-2976, CVE-2024-37890, CVE-2024-37891, CVE-2024-30171, CVE-2024-30172, CVE-2024-29857, CVE-2023-50314, CVE-2024-31882, CVE-2024-35136, CVE-2024-35152, CVE-2024-37529)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Information Disclosure, NULL Pointer Dereference, Denial of Service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 - Versions 11.5.0 - 11.5.9 IBM QRadar SIEM - Versions 7.5 - 7.5.0 UP8 IBM Security QRadar EDR - Versions 3.12 IBM WebSphere Application Server - 9.0, 8.5 IBM WebSphere Application Server Liberty - 17.0.0.3 - 24.0.0.8 IBM WebSphere Hybrid Edition - 5.1 IBM WebSphere Remote Server - Versions 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7165770 • https://www.ibm.com/support/pages/node/7165686 • https://www.ibm.com/support/pages/node/7165685 • https://www.ibm.com/support/pages/node/7165340 • https://www.ibm.com/support/pages/node/7165686 • https://www.ibm.com/support/pages/node/7165882 • https://www.ibm.com/support/pages/node/7165883 • https://www.ibm.com/support/pages/node/7165834

Disclaimer

The information provided are gathered from official vendor websites and portals. FinCSIRT strongly recommends members to apply relevant security fixes immediately to protect systems from potential threats.