



Advisory Alert

Alert Number: AAA20251008 Date: October 8, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	High	Multiple Vulnerabilities
NetApp	High, Medium, Low	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53168, CVE-2025-21791, CVE-2025-38477)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. CVE-2024-53168 - sunrpc: fix one UAF issue caused by sunrpc kernel tcp socket (bsc#1243650). CVE-2025-38477 - net/sched: sch_qfq: Fix race condition on qfq_aggregate (bsc#1247315). CVE-2025-21791 - vrf: use RCU protection in l3mdev_l3_out() SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-202503475-1/

Affected Product	NetApp
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20983, CVE-2024-7840, CVE-2024-8014, CVE-2024-8048, CVE-2025-21583, CVE-2025-21588, CVE-2025-26465, CVE-2025-30722, CVE-2025-50077, CVE-2025-50078, CVE-2025-50079, CVE-2025-50080, CVE-2025-50082, CVE-2025-50083, CVE-2025-50084, CVE-2025-50085, CVE-2025-50086, CVE-2025-50087, CVE-2025-50088, CVE-2025-50091, CVE-2025-50092, CVE-2025-50093, CVE-2025-50094, CVE-2025-50096, CVE-2025-50097, CVE-2025-50098, CVE-2025-50099, CVE-2025-50100, CVE-2025-50101, CVE-2025-50102, CVE-2025-50104, CVE-2025-53023, CVE-2025-5399)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, sensitive information disclosure and addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for VMware vSphere OnCommand Insight OnCommand Workflow Automation SnapCenter NetApp HCI Compute Node (Bootstrap OS) ONTAP tools for VMware vSphere 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/

Affected Product	Red Hat
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22026, CVE-2025-38718)
Description	<p>Red Hat has released security updates addressing multiple vulnerabilities that exist in their products.</p> <p>CVE-2025-22026 - nfsd: don't ignore the return code of svc_proc_register()</p> <p>CVE-2025-38718 - sctp: linearize cloned gso packets in sctp_rcv</p> <p>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.</p>
Affected Products	<p>Red Hat Enterprise Linux for x86_64 10 x86_64</p> <p>Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64</p> <p>Red Hat Enterprise Linux for IBM z Systems 10 s390x</p> <p>Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x</p> <p>Red Hat Enterprise Linux for Power, little endian 10 ppc64le</p> <p>Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le</p> <p>Red Hat Enterprise Linux for ARM 64 10 aarch64</p> <p>Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64</p> <p>Red Hat CodeReady Linux Builder for x86_64 10 x86_64</p> <p>Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le</p> <p>Red Hat CodeReady Linux Builder for ARM 64 10 aarch64</p> <p>Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x</p> <p>Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64</p> <p>Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le</p> <p>Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x</p> <p>Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64</p> <p>Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64</p> <p>Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x</p> <p>Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le</p> <p>Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64</p>
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:17396

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.