



Advisory Alert

Alert Number: **AAA20261006** Date: October 6, 2026

Document Classification Level : **Public Circulation Permitted | Public**

Information Classification Level : **TLP: WHITE**

Overview

Vendor	Severity	Vulnerability
IBM	Critical	Multiple Vulnerabilities
Zyxel Networks	High	Command Injection Vulnerability
SUSE	High	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities
Ubuntu	Medium	Multiple Vulnerabilities
Zabbix	Medium, Low	Multiple Vulnerabilities

Description

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42581, CVE-2026-42584, CVE-2026-39830, CVE-2026-39831, CVE-2026-39832, CVE-2026-39833, CVE-2026-39834, CVE-2026-42508, CVE-2026-46595)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	- IBM Fusion - Versions 2.9.0 - 2.13.1 - IBM Fusion HCI - Versions 2.10.0 - 2.13.1 - IBM Storage Scale Version 6.0.1.0 - IBM Storage Scale Versions 5.2.3.0 - 5.2.3.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7291296 https://www.ibm.com/support/pages/node/7290896

Vendor	Zyxel Networks
Severity	High
Affected Vulnerability	Command Injection Vulnerability (CVE-2023-20820)
Description	Zyxel Networks has released a security update addressing a vulnerability that exists in their products. CVE-2023-20820: Zyxel has released patches for specific firmware versions of certain DSL/Ethernet CPE, fiber ONTs, and Wireless Extenders devices using MediaTek WiFi chipsets to address a post-authentication command injection vulnerability. Users are strongly advised to install these patches to ensure optimal protection. Zyxel Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DSL/Ethernet CPE: - Versions 5.50(ABVY.8.2)C0 and earlier: DX3300-T0, DX3300-T1, DX3301-T0, EX3300-T0, EX3300-T1, and EX3301-T0 - Versions 5.44(ACHR.6)C0 and earlier: EX3500-T0 and EX3501-T0 - Versions 5.70(ACIF.3.2)C0 and earlier: EX3600-T0 - Versions 5.70(ACEG.5.7)C0 and earlier: EX5512-T0 - Versions 5.70(ACDZ.6.2)C0 and earlier: EX5601-T0 and EX5601-T1 Fiber ONTs: - Versions 5.44(ACKB.0.8)C0 and earlier: PX5301-T0 Wireless Extenders: - Versions 5.70(ACKA.2.1)C0 and earlier: WE3300-00 - Versions 5.50(ABVL.5.1)C0 and earlier: WX3100-T0 - Versions 5.70(ACEB.6.2)C0 and earlier: WX5600-T0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-command-injection-vulnerability-in-the-wifi-ssid-field-of-certain-dsl-ethernet-cpe-fiber-onts-and-wireless-extenders-10-06-2026

Vendor	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-39830, CVE-2026-42581, CVE-2026-42584, CVE-2026-46116, CVE-2026-63802, CVE-2026-63888, CVE-2026-63912, CVE-2026-63917, CVE-2026-63920, CVE-2026-63921, CVE-2026-63944, CVE-2026-63971, CVE-2026-63994, CVE-2026-64000, CVE-2026-64011, CVE-2026-64114, CVE-2026-64121, CVE-2026-64189, CVE-2026-68121, CVE-2026-68202, CVE-2026-74394, CVE-2026-74612)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7 openSUSE Leap 15.4 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	- https://www.suse.com/support/update/announcement/2026/suse-su-20264471-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264450-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264497-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264498-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264495-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264507-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264489-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264513-1/ - https://www.suse.com/support/update/announcement/2026/suse-su-20264514-1/

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39994, CVE-2025-40242, CVE-2023-54048, CVE-2022-50756, CVE-2026-23105, CVE-2026-45856, CVE-2026-45861, CVE-2026-46319, CVE-2026-53049, CVE-2026-52972, CVE-2026-53230, CVE-2026-53270, CVE-2026-63829, CVE-2026-63794, CVE-2026-63992, CVE-2026-63994, CVE-2026-68432, CVE-2026-72052, CVE-2026-72255, CVE-2026-74516, CVE-2026-74569, CVE-2026-74669, CVE-2026-74744, CVE-2026-74746, CVE-2026-80921, CVE-2026-89481, CVE-2026-89972, CVE-2026-90227, CVE-2026-97417)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:75747

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46340, CVE-2026-6790, CVE-2026-50020, CVE-2026-33870, CVE-2026-41417, CVE-2026-42580, CVE-2026-42585, CVE-2026-42587, CVE-2026-45416, CVE-2026-39827, CVE-2026-39828, CVE-2026-39829, CVE-2026-39835, CVE-2026-46597, CVE-2026-46598, CVE-2026-14437, CVE-2026-14469, CVE-2026-14375, CVE-2026-76905, CVE-2026-17033)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Scale Container Native and CSI Versions: 6.0.1.0 / CSI 3.1.0 5.2.3.0 - 5.2.3.9 / CSI 2.14.0 - 2.14.7 IBM Fusion - Versions 2.9.0 - 2.13.1 IBM Fusion HCI - Versions 2.10.0 - 2.13.1 IBM Storage Scale Version 6.0.1.0 IBM Storage Scale Versions 5.2.3.0 - 5.2.3.9 IBM Security QRadar Log Management AQL Plugin Versions - 1.0.0 - 1.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7291295 https://www.ibm.com/support/pages/node/7291296 https://www.ibm.com/support/pages/node/7291325 https://www.ibm.com/support/pages/node/7290896 https://www.ibm.com/support/pages/node/7290857

Vendor	Ubuntu
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53221, CVE-2026-53131, CVE-2025-38724)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in their products. CVE-2026-53221: In the Linux kernel, the following vulnerability has been resolved: ip6_vti: fix incorrect tunnel matching in vti6_tnl_lookup() In vti6_tnl_lookup(), when an exact match for a tunnel fails, the code falls back to searching for wildcard tunnels: - Tunnels matching the packet’s local address, with any remote address wildcard remote). - Tunnels matching the packet’s remote address, with any local address (wildcard local). However, vti6 stores all these different types of tunnels in the same hash table (ip6n->tnls_r_l) prone to hash collisions. The bug is that the fallback search loops in vti6_tnl_lookup() were missing checks to ensure that the candidate tunnel actually has a wildcard address. CVE-2026-53131: In the Linux kernel, the following vulnerability has been resolved: netfilter: require Ethernet MAC header before using eth_hdr() `ip6t_eui64`, `xt_mac`, the `bitmap:ip,mac`, `hash:ip,mac`, and `hash:mac` ipset types, and `nf_log_syslog` access `eth_hdr(skb)` after either assuming that the skb is associated with an Ethernet device or checking only that the `ETH_HLEN` bytes at `skb_mac_header(skb)` lie between `skb->head` and `skb->data`. Make these paths first verify that the skb is associated with an Ethernet device, that the MAC header was set, and that it spans at least a full Ethernet header before accessing `eth_hdr(skb)`. CVE-2025-38724: In the Linux kernel, the following vulnerability has been resolved: nfsd: handle get_client_locked() failure in nfsd4_setclientid_confirm() Lei Lu recently reported that nfsd4_setclientid_confirm() did not check the return value from get_client_locked(). A SETCLIENTID_CONFIRM could race with a confirmed client expiring and fail to get a reference. That could later lead to a UAF. Fix this by getting a reference early in the case where there is an extant confirmed client. If that fails then treat it as if there were no confirmed client found at all. In the case where the unconfirmed client is expiring, just fail and return the result from get_client_locked(). Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8851-3

Vendor	Zabbix
Severity	Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-59788, CVE-2026-59787, CVE-2026-59786, CVE-2026-59785, CVE-2026-59783, CVE-2026-59782)
Description	Zabbix has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Zabbix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Frontend Versions: 6.0.0-6.0.47 7.0.0-7.0.28 7.4.0-7.4.12 Server, Proxy Versions: 6.0.0-6.0.47 7.0.0-7.0.28 7.4.0-7.4.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.zabbix.com/security_advisories?sortBy=zabbix_web_security_advisories%2Fsort%2Fpublished_int%3Adesc&query=Z#modal

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.