Advisory Alert

Alert Number: AAA20260113 **Date:** January 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	OS Command Injection Vulnerability
SUSE	**High**	Wifi Driver UAF Vulnerability
Red Hat	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2023-51385)
Description	IBM has released security updates addressing a vulnerability that exists in their Access management Products. **CVE-2023-51385 -** OS command injection can occur if a username or hostname contains shell metacharacters that are referenced by expansion tokens, potentially allowing arbitrary command execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Verify Identity Access (11.0–11.0.1) IBM Security Verify Access (10.0–10.0.9)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7256856

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Wi-Fi Driver UAF Vulnerability (CVE-2023-53574)
Description	SUSE has released security updates addressing a vulnerability that exists in the Realtek Wi-Fi driver subsystem of their products. **CVE-2023-53574** - A flaw in the rtw88 WiFi driver occurs during the unloading process where it fails to properly delete timers and free socket buffer (skb) queues. This can lead to use-after-free or memory leak conditions, which a local attacker could exploit to cause a system crash or potentially execute arbitrary code. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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-20260107-1/

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23142, CVE-2025-39806, CVE-2025-39981, CVE-2025-39983, CVE-2025-40176, CVE-2025-68287)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Linux Kernel of 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 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 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 - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder 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 Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0457

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51767, CVE-2023-51384, CVE-2025-26465, CVE-2023-48795, CVE-2023-38408)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Verify Identity Access (11.0–11.0.1) IBM Security Verify Access (10.0–10.0.9)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7256856

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.