Advisory Alert

Alert Number: AAA20261103 **Date:** November 3, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Barracuda	**High**	Multiple Vulnerabilities
Zyxel Networks	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71066, CVE-2026-43051, CVE-2026-46086, CVE-2026-53073, CVE-2026-53224, CVE-2026-53246, CVE-2026-63875, CVE-2026-74556, CVE-2026-90227, CVE-2026-98432)
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 Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:94109

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-25289, CVE-2026-25285, CVE-2026-45447, CVE-2026-34182, CVE-2026-45445, CVE-2026-7383, CVE-2026-9076, CVE-2026-34180, CVE-2026-42766, CVE-2026-42770, CVE-2026-45446)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.

Affected Products	• Alienware 15 DA15260 - Versions prior to 1.4.0
	• Dell 14 Plus 2-in-1 DB04255 - Versions prior to 1.14.0
	• Dell 14 Plus DB14255 - Versions prior to 1.14.0
	• Dell 16 Plus DB16255 - Versions prior to 1.14.0
	• Versions prior to 2.17.0:
	  ○ Latitude 5455
	  ○ Latitude 7455
	  ○ Inspiron 14 7441
	  ○ Inspiron 14 5441
	  ○ XPS 13 9345

Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000528834/dsa-2026-321-security-update-for-dell-client-platform-for-a-qualcomm-chipset-vulnerability • https://www.dell.com/support/kbdoc/en-us/000501830/dsa-2026-285-security-update-for-dell-client-platform-for-a-qualcomm-chipset-vulnerability • https://www.dell.com/support/kbdoc/en-us/000499671/dsa-2026-366-security-update-for-dell-client-platform-bios-for-multiple-insyde-bios-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-78663, CVE-2026-42579, CVE-2026-42581, CVE-2026-42584, CVE-2026-75595, CVE-2026-45674, CVE-2026-55976, CVE-2026-2332, CVE-2026-10050, CVE-2026-90711)
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 QRadar Data Synchronization App Versions - 1.0.0 - 4.0.0 • QRadar User Behavior AnalyticsVersions - 1.0.0 - 6.0.1 • IBM Security QRadar Log Management AQL Plugin Versions - 1.0.0 - 1.1.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7295131 https://www.ibm.com/support/pages/node/7295130 https://www.ibm.com/support/pages/node/7295132

Vendor	**Barracuda**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-116606, CVE-2026-111560)
Description	Barracuda has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-116606:** An authentication bypass in Barracuda Email Security Gateway versions earlier than 9.4.0.030 allows an unauthenticated remote attacker to invoke a configuration-import function and restore a crafted, compatible backup archive, resulting in unauthorized modification of the appliance's global configuration. **CVE-2026-111560:** Improper neutralization of shell metacharacters in the timezone configuration field in certain Barracuda appliance products using common Barracuda code allows an authenticated administrator to inject OS commands that execute with root privileges when the crafted timezone value is subsequently processed. Barracuda advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Email Security Gateway (ESG) Load Balancer Application Delivery Controller (ADC) Message Archiver (BMA) WAF Control Center (WCC) Web Application Firewall (WAF) Web Security Gateway (WSG)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://trust.barracuda.com/security/pre-authentication-authorization-bypass-command-injection

Vendor	**Zyxel Networks**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-107441, CVE-2026-76955)
Description	Zyxel Networks 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. Zyxel Networks advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-out-of-bounds-write-vulnerability-in-gs1900-series-switches-11-03-2026 • https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-buffer-overflow-vulnerability-in-certain-aps-fwa7-and-security-routers-11-03-2026

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Versions prior to 2.17.0: • Latitude 5455 • Latitude 7455 • Inspiron 14 7441 • Inspiron 14 5441 • XPS 13 9345 PowerScale InsightIQ Versions: • Versions 6.3.0 through 6.4.0 • Version 6.4.0 • Versions 5.1.0 through 6.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000528934/dsa-2026-480-security-update-for-dell-powerscale-insightiq-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000528823/dsa-2026-180-security-update-for-dell-client-platform-for-multiple-qualcomm-chipset-driver-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000528829/dsa-2026-191-security-update-for-dell-client-platform-for-a-qualcomm-chipset-vulnerability • https://www.dell.com/support/kbdoc/en-us/000516263/dsa-2026-449-security-update-for-dell-client-platform-for-a-qualcomm-chipset-vulnerability

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53016, CVE-2026-53381, CVE-2026-63968, CVE-2026-64217, CVE-2026-68426, CVE-2026-72262, CVE-2026-74469, CVE-2026-74669, CVE-2026-89544, CVE-2026-89551, CVE-2026-89674, CVE-2026-98432)
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 Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 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 openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20265012-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265002-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265006-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265015-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265019-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265016-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265030-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265033-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20265034-1/

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-98432, CVE-2026-111497, CVE-2026-63996, CVE-2026-63987, CVE-2026-63922, CVE-2026-63924, CVE-2026-64109, CVE-2026-72083, CVE-2026-74283, CVE-2026-93787)
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 the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	RHEL 10 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, s390x, x86_64 • Hidden Content: x86_64 RHEL 10.2: • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 • 4 Years of Updates/Support: aarch64, ppc64le, s390x, x86_64 • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 9 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, s390x, x86_64 RHEL 9.8: • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • 4 Years of Updates: aarch64, s390x • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 9.4: • Advanced Update Support (AUS): x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • 4 Years of Updates: aarch64, s390x • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 8 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, x86_64 RHEL 8.10: • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:93775 https://access.redhat.com/errata/RHSA-2026:93550 https://access.redhat.com/errata/RHSA-2026:93911 https://access.redhat.com/errata/RHSA-2026:93930 https://access.redhat.com/errata/RHSA-2026:93436

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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 QRadar Data Synchronization App Versions - 1.0.0 - 4.0.0 • QRadar User Behavior Analytics Versions - 1.0.0 - 6.0.1 • IBM Security QRadar Log Management AQL Plugin Versions - 1.0.0 - 1.1.11 • NTA Versions 1.0.0 - 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7295133 https://www.ibm.com/support/pages/node/7295131 https://www.ibm.com/support/pages/node/7295130 https://www.ibm.com/support/pages/node/7295132

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.