Advisory Alert

Alert Number: AAA20260217 **Date:** February 17, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Stack-Based Buffer Overflow Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
HPE	**Low**	Local Privilege Escalation Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Stack-Based Buffer Overflow Vulnerability (CVE-2025-15467)
Description	IBM has released security updates addressing a vulnerability that exists in their Products. **CVE-2025-15467 -** A critical vulnerability allows a specially crafted encrypted CMS message to trigger a stack buffer overflow when processed with AEAD ciphers like AES-GCM. The flaw occurs because the system copies an attacker-controlled initialization vector into a fixed-size memory buffer without validating its length. This can crash affected services (DoS) or potentially enable remote code execution, even without valid encryption keys. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service versions 2.0.0 - 2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7260902

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40129, CVE-2025-40186, CVE-2025-38111, CVE-2025-38352, CVE-2025-39742)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260561-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260560-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260557-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260556-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260555-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260554-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260551-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260550-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260548-1/

Affected Product	**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 affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service (versions 2.0.0 - 2.1.0) IBM Db2 Server versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7257681 • https://www.ibm.com/support/pages/node/7257692 • https://www.ibm.com/support/pages/node/7260902

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37882, CVE-2025-38415, CVE-2025-38730, CVE-2025-39760, CVE-2025-39933, CVE-2025-40269, CVE-2025-40271, CVE-2025-40304, CVE-2025-68349, CVE-2025-38051, CVE-2025-38383, CVE-2025-40294, CVE-2025-38349)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Linux kernel component 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 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 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 CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:2766 • https://access.redhat.com/errata/RHSA-2026:2761 • https://access.redhat.com/errata/RHSA-2026:2759

Affected Product	**HPE**
Severity	**Low**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2025-31648)
Description	HPE has released security updates addressing a vulnerability that exists in their products. **CVE-2025-31648** - A potential security vulnerability in HPE ProLiant DL/ML/XD, Synergy, Edgeline, MicroServer, and Alletra servers using certain Intel processors could be locally exploited to allow escalation of privilege vulnerability. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant Compute DL320 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL340 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL360 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL380 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL380a Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute DL580 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute ML350 Gen12 - Prior to v1.60_01-09-2026 HPE ProLiant Compute XD230 - Prior to v1.60_01-09-2026 HPE Synergy 480 Gen12 Compute Module - Prior to v1.60_01-09-2026 HPE Alletra Storage Server 4210 - Prior to v1.60_01-09-2026 HPE ProLiant DL20 Gen11 - Prior to v2.40_02-05-2026 HPE ProLiant DL110 Gen11 - Prior to v2.80_01_29_2026 HPE ProLiant DL320 Gen11 Server - Prior to v2.80_01_29_2026 HPE ProLiant DL360 Gen11 Server - Prior to v2.80_01_29_2026 HPE ProLiant DL380 Gen11 Server - Prior to v2.80_01_29_2026 HPE ProLiant DL380a Gen11 - Prior to v2.80_01_29_2026 HPE ProLiant DL560 Gen11 - Prior to v2.80_01_29_2026 HPE ProLiant ML30 Gen11 - Prior to v2.40_02-05-2026 HPE ProLiant ML110 Gen11 - Prior to v2.80_01_29_2026 HPE ProLiant ML350 Gen11 Server - Prior to v2.80_01_29_2026 HPE ProLiant MicroServer Gen11 - Prior to v2.40_02-05-2026 HPE Alletra 4110 - Prior to v2.80_01_29_2026 HPE Alletra 4120 - Prior to v2.80_01_29_2026 HPE Alletra 4140 - Prior to v2.80_01_29_2026 HPE Synergy 480 Gen11 Compute Module - Prior to v2.80_01_29_2026 HPE Compute Edge Server e930t - Prior to v2.80_01_29_2026 HPE Apollo 4200 Gen10 Plus/HPE ProLiant XL420 Gen10 Plus Server - Prior to v2.60_02-05-2026 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.60_02-05-2026 HPE ProLiant DL20 Gen10 Plus server - Prior to v2.60_02-05-2026 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.60_02-05-2026 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.60_02-05-2026 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.60_02-05-2026 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.60_02-05-2026 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.60_02-05-2026 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.60_02-05-2026 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.60_02-05-2026 HPE Edgeline e920 Server Blade - Prior to v2.60_02-05-2026 HPE Edgeline e920d Server Blade - Prior to v2.60_02-05-2026 HPE Edgeline e920t Server Blade - Prior to v2.60_02-05-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05008en_us&docLocale=en_US

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.