Advisory Alert

Alert Number: AAA20260519 **Date:** May 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Path Traversal Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Privilege Escalation Vulnerability
SUSE	**High**	Multiple Vulnerabilities
F5	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium**	Multiple Vulnerabilities
HP	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2026-27699)
Description	HPE has released a security update addressing a vulnerability that exists in their product. **CVE-2026-27699**: The `basic-ftp` FTP client library for Node.js contains a path traversal vulnerability (CWE-22) in versions prior to 5.2.0 in the `downloadToDir()` method. A malicious FTP server can send directory listings with filenames containing path traversal sequences (`../`) that cause files to be written outside the intended download directory. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Unified OSS Console (UOC) UOC Version 3.1.20 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05056en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40674, CVE-2026-27459, CVE-2025-62718, CVE-2026-4800, CVE-2026-4277, CVE-2026-33701, CVE-2026-29045, CVE-2026-33186, CVE-2026-29063, CVE-2026-33228, CVE-2025-59059, CVE-2025-68121)
Description	IBM has released security updates addressing multiple vulnerability that exist in their product. 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 - Data Protect – Versions 2.0.0-2.1.3 IBM Fusion – Versions 2.9.0 - 2.12.1 IBM Fusion HCI – Versions 2.10.0 - 2.12.1 Data Cataloging – Versions 2.1.8 - 2.5.1 IBM Storage Defender - Resiliency Service – Versions 2.0.0 - 2.1.3 IBM® Db2® on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data Versions: • v4.8 • v5.0 • v5.1 • v5.2 • v5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7272819 https://www.ibm.com/support/pages/node/7272780 https://www.ibm.com/support/pages/node/7272566 https://www.ibm.com/support/pages/node/7273312

ffected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-43284)
Description	Red Hat has released a security update addressing a vulnerability that exists in the kernel of their products. **CVE-2026-43284:** A flaw was found in the Linux kernel's xfrm-ESP and RxRPC subsystems. Unsafe in-place cryptographic processing of shared socket buffer fragments allows a low-privileged local attacker to corrupt page-cache contents of readable files, including sensitive system files, and gain root privileges. The xfrm-ESP variant requires unprivileged user or network namespace creation, while the RxRPC variant depends on the rxrpc module being available on the target system. 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 Power, little endian - Extended Update Support 9.6 ppc64le 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 Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:18025

ffected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54518 CVE-2026-43284 CVE-2026-43500 CVE-2026-46300 CVE-2026-46333)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel of 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	openSUSE Leap 15.4 openSUSE Leap 15.5 openSUSE Leap 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 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 Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20261917-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261959-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261960-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20261994-1/

ffected Product	**F5**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43284, CVE-2024-50275)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. **CVE-2026-43284:** In the Linux kernel, the following vulnerability has been resolved: arm64/sve: Discard stale CPU state when handling SVE traps The logic for handling SVE traps manipulates saved FPSIMD/SVE state incorrectly, and a race with preemption can result in a task having TIF_SVE set and TIF_FOREIGN_FPSTATE clear even though the live CPU state is stale (e.g. with SVE traps enabled). **CVE-2024-50275:** In the Linux kernel, the following vulnerability has been resolved: RDMA/bnxt_re: Fix a bug while setting up Level-2 PBL pages Avoid memory corruption while setting up Level-2 PBL pages for the non MR resources when num_pages > 256K. There will be a single PDE page address (contiguous pages in the case of > PAGE_SIZE), but, current logic assumes multiple pages, leading to invalid memory access after 256K PBL entries in the PDE. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Traffix SDC 5.x – Versions 5.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000153108 https://my.f5.com/manage/s/article/K000153097

ffected Product	**HPE**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12758, CVE-2025-64945, CVE-2026-25639, CVE-2026-26996, CVE-2026-27601, CVE-2026-27903, CVE-2026-27904)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Unified OSS Console (UOC) UOC Version 3.1.20 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05056en_us&docLocale=en_US

Affected Product	**HP**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31317, CVE-2022-23817, CVE-2021-46747, CVE-2023-31316, CVE-2024-36333, CVE-2023-31309, CVE-2025-0044, CVE-2025-66664, CVE-2025-66660, CVE-2022-23826, CVE-2021-26380)
Description	HP has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HP 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://support.hp.com/us-en/document/ish_14934878-14934908-16/hpsbhf04121

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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerVC – Versions 2.2.1.2, 2.3.0, 2.3.1 & 2.3.2 IBM WebSphere Remote Server – Versions 8.5, 9.0 & 9.1 IBM Fusion – Versions 2.9.0 - 2.12.1 IBM Fusion HCI – Versions 2.10.0 - 2.12.1 Data Cataloging – Versions 2.1.8 - 2.5.1 IBM Storage Defender - Resiliency Service – Versions 2.0.0 - 2.1.3 Platform Navigator in IBM Cloud Pak for Integration (CP4I) – Versions 16.1.0 to 16.1.0.22, 16.1.1, 16.1.2, 16.1.3.0 to 16.1.3.5 Automation Assets in IBM Cloud Pak for Integration (CP4I) – Versions 4.0.0-sc2 to 4.0.19-sc2, 4.1.0, 4.2.0, 4.3.0 to 4.3.3 IBM Storage Defender - Data Protect – Versions 2.0.0-2.1.3 IBM® Db2® on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data Versions: • v4.8 • v5.0 • v5.1 • v5.2 • v5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7273275 • https://www.ibm.com/support/pages/node/7273278 • https://www.ibm.com/support/pages/node/7273329 • https://www.ibm.com/support/pages/node/7272780 • https://www.ibm.com/support/pages/node/7272566 • https://www.ibm.com/support/pages/node/7273312 • https://www.ibm.com/support/pages/node/7273289 • https://www.ibm.com/support/pages/node/7272773 • https://www.ibm.com/support/pages/node/7272566 • https://www.ibm.com/support/pages/node/7272819 • https://www.ibm.com/support/pages/node/7273312

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.