Advisory Alert

Alert Number: AAA20250116 **Date:** January 16, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Authenticated Remote Arbitrary Code Execution Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
F5	Medium	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to memory leak, data corruption, use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4, 15.5, 15.6 Public Cloud Module 15-SP6 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250132-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250131-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250124-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250123-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250117-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250115-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250114-1/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Authenticated Remote Arbitrary Code Execution Vulnerabilities (CVE-2025-23051, CVE-2025-23052)
Description	HPE has released security updates addressing multiple Authenticated Remote Arbitrary Code Execution vulnerabilities that exist in AOS-8 and AOS-10 Command Line Interfaces. **CVE-2025-23051** - An authenticated parameter injection vulnerability exists in the web-based management interface of the AOS-8 and AOS-10 Operating Systems. Successful exploitation could allow an authenticated user to leverage parameter injection to overwrite arbitrary system files. **CVE-2025-23052** - Authenticated command injection vulnerability in the command line interface of a network management service. Successful exploitation of this vulnerability could allow an attacker to execute arbitrary commands as a privileged user on the underlying operating system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following HPE Aruba Networking products • Mobility Conductor • Mobility Controllers • WLAN and SD-WAN Gateways Managed by HPE Aruba Networking Central Running on, • AOS-10.4.x.x: 10.4.1.4 and below • AOS-8.12.x.x: 8.12.0.2 and below • AOS-8.10.x.x: 8.10.0.14 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04723en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50264, CVE-2024-49967, CVE-2024-53057)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel (Real-time). Malicious users could exploit these vulnerabilities to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7169-5

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21217, CVE-2024-21208, CVE-2024-10917, CVE-2024-9143, CVE-2024-21147, CVE-2024-21145, CVE-2024-21140, CVE-2024-21144, CVE-2024-21138, CVE-2024-21131, CVE-2024-27267, CVE-2024-21085, CVE-2024-21012, CVE-2024-3933, CVE-2024-21094, CVE-2024-21011, CVE-2023-38264)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in Db2 Query Management Facility. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, Security Restrictions Bypass, Denial Of Service, high integrity impact. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Db2 Query Management Facility 13.1.1 and 13.1.2 DB2 Query Management Facility for z/OS 12.2 and 13.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7178758 • https://www.ibm.com/support/pages/node/7168925 • https://www.ibm.com/support/pages/node/7178756 • https://www.ibm.com/support/pages/node/7156671

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-3859, CVE-2019-3860)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2019-3859** - An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the _libssh2_packet_require and _libssh2_packet_requirev functions. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. **CVE-2019-3860** - An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SFTP packets with empty payloads are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (AFM) Versions - 15.1.0 - 15.1.10, 16.1.0 - 16.1.5, 17.1.0 - 17.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000149288

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.