TLP: WHITE

Advisory Alert

Alert Number: **AAA20250804** **Date:** **August 4, 2025**

Document Classification Level	:	Public Circulation Permitted | Public
Information Classification Level	:	TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High**	Multiple Vulnerabilities
Sophos	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-49569, CVE-2022-46337, CVE-2022-1996, CVE-2020-9546, CVE-2019-16943, CVE-2019-17531, CVE-2020-9547, CVE-2019-16942, CVE-2020-9548, CVE-2020-10968, CVE-2020-11111, CVE-2020-11112, CVE-2020-11113, CVE-2020-10673, CVE-2020-10969, CVE-2020-10672, CVE-2020-14062, CVE-2020-14195, CVE-2020-14061, CVE-2020-24750, CVE-2021-20190, CVE-2020-14060, CVE-2020-11620, CVE-2020-36179, CVE-2020-36180, CVE-2020-36181, CVE-2020-36182, CVE-2020-36183, CVE-2020-36184, CVE-2020-36185, CVE-2020-36186, CVE-2020-11619, CVE-2020-36188, CVE-2020-36189, CVE-2020-24616, CVE-2020-36187, CVE-2022-36364,CVE-2024-1597, CVE-2025-30472)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Db2 Server, IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data. These vulnerabilities could be exploited by malicious users to cause Arbitrary Code Execution, directory traversal, Data Modification, Bypass Security Restrictions. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.5.0 - 11.5.9 and 12.1.0 - 12.1.2 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions : • v3.5 through refresh 10 • v4.0 through refresh 9 • v4.5 through refresh 3 • v4.6 through refresh 6 • v4.7 through refresh 4 • v4.8 through refresh 4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7155078 • https://www.ibm.com/support/pages/node/7240977

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49138, CVE-2022-49770, CVE-2023-52923, CVE-2023-52927, CVE-2024-26643, CVE-2024-53057, CVE-2024-53164, CVE-2024-57947, CVE-2025-37797, CVE-2025-38079, CVE-2025-38181, CVE-2025-38200, CVE-2025-38206, CVE-2025-38212, CVE-2025-38213, CVE-2025-38257, CVE-2025-38289)
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 system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 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 15 SP5 LTSS 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/2025/suse-su-202502588-1/

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1094, CVE-2024-55549)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-1094** - Multiple NetApp products incorporate PostgreSQL. PostgreSQL versions prior to 17.3, prior to 16.7, prior to 15.11, prior to 14.16, and prior to 13.19 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). **CVE-2024-55549** - Multiple NetApp products incorporate libxslt. Libxslt versions prior to 1.1.43 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Brocade SAN Navigator (SANnav) ONTAP 9 ONTAP tools for VMware vSphere 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250221-0010 • https://security.netapp.com/advisory/ntap-20250613-0007

Affected Product	**Sophos**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-13972, CVE-2025-7433, CVE-2025-7472)
Description	Sophos has released security updates addressing multiple vulnerabilities that exist in Sophos Intercept X for Windows. **CVE-2024-13972** - A vulnerability related to registry permissions in the Intercept X for Windows updater can lead to a local user gaining system level privileges during a product upgrade. The issue was discovered and responsibly disclosed to Sophos by an external security researcher. **CVE-2025-7433** - A local privilege escalation vulnerability, allowing arbitrary code execution, was discovered in the Device Encryption component of Sophos Intercept X for Windows. The issue was discovered and responsibly disclosed to Sophos by an external security researcher. **CVE-2024-13972** - A local privilege escalation vulnerability in the Intercept X for Windows installer can lead to a local user gaining system level privileges, if the installer is run as SYSTEM. The issue was discovered and responsibly disclosed to Sophos by an external security researcher via the Sophos bug bounty program. Sophos advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Sophos Intercept X for Windows prior to Core Agent version 2024.3.2 Sophos Intercept X for Windows Central Device Encryption prior to version 2025.1 Sophos Intercept X for Windows Installer prior to version 1.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sophos.com/en-us/security-advisories/sophos-sa-20250717-cix-lpe

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM and Db2 modules. These vulnerabilities could be exploited by malicious users to cause Denial of Service, data modification, Information Disclosure, authorization bypass, XSS, Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP12 IF03 IBM Db2 Intelligence Center 1.1.0.0 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data versions : • v3.5 through refresh 10 • v4.0 through refresh 9 • v4.5 through refresh 3 • v4.6 through refresh 6 • v4.7 through refresh 4 • v4.8 through refresh 4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7155078 • https://www.ibm.com/support/pages/node/7241303 • https://www.ibm.com/support/pages/node/7241292

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.