Advisory Alert

Alert Number: AAA20251216 **Date:** December 16, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
pgAdmin	**Critical**	Command Injection Vulnerability
SUSE	**High**	Multiple Vulnerabilities
NetApp	**High**	Security Update
IBM	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**pgAdmin**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2025-13780)
Description	PostgreSQL has released a security update addressing a command injection vulnerability that is present in pgAdmin. **CVE-2025-13780:** pgAdmin versions up to 9.10 are affected by a Remote Code Execution (RCE) vulnerability that occurs when running in server mode and performing restores from PLAIN-format dump files. This issue allows attackers to inject and execute arbitrary commands on the server hosting pgAdmin, posing a critical risk to the integrity and security of the database management system and underlying data. PostgreSQL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	pgAdmin versions up to 9.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.pgadmin.org/

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50253, CVE-2023-53676, CVE-2025-21710, CVE-2025-37916, CVE-2025-38359, CVE-2025-39788, CVE-2025-39805, CVE-2025-39819, CVE-2025-39822, CVE-2025-39859, CVE-2025-39944, CVE-2025-39980, CVE-2025-40001, CVE-2025-40021, CVE-2025-40027, CVE-2025-40030, CVE-2025-40038, CVE-2025-40040, CVE-2025-40047, CVE-2025-40048, CVE-2025-40055, CVE-2025-40059, CVE-2025-40064, CVE-2025-40070, CVE-2025-40074, CVE-2025-40075, CVE-2025-40080, CVE-2025-40083, CVE-2025-40086, CVE-2025-40098, CVE-2025-40105, CVE-2025-40107, CVE-2025-40109, CVE-2025-40110, CVE-2025-40111, CVE-2025-40115, CVE-2025-40116, CVE-2025-40118, CVE-2025-40120, CVE-2025-40121, CVE-2025-40127, CVE-2025-40129, CVE-2025-40139, CVE-2025-40140, CVE-2025-40141, CVE-2025-40149, CVE-2025-40154, CVE-2025-40156, CVE-2025-40157, CVE-2025-40159, CVE-2025-40164, CVE-2025-40168, CVE-2025-40169, CVE-2025-40171, CVE-2025-40172, CVE-2025-40173, CVE-2025-40176, CVE-2025-40180, CVE-2025-40183, CVE-2025-40185, CVE-2025-40186, CVE-2025-40188, CVE-2025-40194, CVE-2025-40198, CVE-2025-40200, CVE-2025-40204, CVE-2025-40205, CVE-2025-40206, CVE-2025-40207)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 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 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20254393-1/

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-47906)
Description	NetApp has released a security update addressing a vulnerability that exists in Golang which is incorporate by multiple NetApp products. **CVE-2025-47906:** Golang versions prior to 1.23.12 and 1.24.0 prior to 1.24.6 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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetApp Kubernetes Monitoring Operator
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20251024-0005

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42302, CVE-2024-42294, CVE-2024-50058, CVE-2024-26782, CVE-2024-26900, CVE-2024-4741, CVE-2024-43855, CVE-2024-26725, CVE-2024-2511, CVE-2024-42316, CVE-2024-41012, CVE-2024-41020, CVE-2024-36930, CVE-2024-26734, CVE-2024-42090, CVE-2024-46697, CVE-2025-50106, CVE-2025-30749, CVE-2025-30754, CVE-2025-21587, CVE-2025-30698, CVE-2025-66200, CVE-2025-59375, CVE-2025-65082, CVE-2025-59775, CVE-2025-58098, CVE-2024-26708)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS), Unauthorized Access, Information Disclosure and Server-Side Request Forgery (SSRF). IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Scale System 6.2.0.0 - 6.2.3.2 IBM Storage Insights - Data Collector versions 20251030-0236 IBM HTTP Server 8.5 and 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7254807 • https://www.ibm.com/support/pages/node/7254159 • https://www.ibm.com/support/pages/node/7254766

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40018, CVE-2025-39964, CVE-2025-38666, CVE-2025-21855, CVE-2025-21811, CVE-2025-21722, CVE-2025-21715, CVE-2024-53217, CVE-2024-53112, CVE-2024-50179, CVE-2024-50095, CVE-2024-50067, CVE-2024-49935, CVE-2022-49026, CVE-2021-47634, CVE-2021-47385, CVE-2021-47269, CVE-2021-47146, CVE-2025-39993, CVE-2025-37958)
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu versions 14.04, 16.04, 22.04, and 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7930-1 • https://ubuntu.com/security/notices/USN-7931-1

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.