Advisory Alert

Alert Number:	AAA20250129	Date:	January 29, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	High	Unauthenticated Blind SQL Injection Vulnerability
SUSE	High	Multiple Vulnerabilities
Ubuntu	High, Medium	Multiple Vulnerabilities
HPE	Medium	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Unauthenticated Blind SQL Injection Vulnerability (CVE-2025-22217)
Description	Broadcom has released security update addressing an unauthenticated Blind SQL Injection Vulnerability in VMware Avi Load Balancer. A malicious user with network access may be able to use specially crafted SQL queries to gain database access. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Avi Load Balancer 30.1.1 VMware Avi Load Balancer 30.1.2 VMware Avi Load Balancer 30.2.1 VMware Avi Load Balancer 30.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25346

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52752, CVE-2024-35949, CVE-2024-36979, CVE-2024-40909, CVE-2024-40920, CVE-2024-40921, CVE-2024-40954, CVE-2024-41057, CVE-2024-43861, CVE-2024-50264)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause memory leak, Denial of Service, Use-after-Free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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/2025/suse-su-20250269-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250268-1/

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public   Report incidents to incident@fincsirt.lk   TLP: WHITE

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Arbitrary Code Execution. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.10 Ubuntu 24.04 LTS Ubuntu 22.04 LTS Ubuntu 20.04 LTS Ubuntu 18.04 ESM Ubuntu 16.04 ESM Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	- https://ubuntu.com/security/notices/USN-7239-1 - https://ubuntu.com/security/notices/USN-7238-1 - https://ubuntu.com/security/notices/USN-7237-1 - https://ubuntu.com/security/notices/USN-7236-1 - https://ubuntu.com/security/notices/USN-7235-1 - https://ubuntu.com/security/notices/USN-7234-1 - https://ubuntu.com/security/notices/USN-7233-1 - https://ubuntu.com/security/notices/USN-7232-1 - https://ubuntu.com/security/notices/USN-7231-1 - https://ubuntu.com/security/notices/USN-7206-3

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23053 , CVE-2025-23054 , CVE-2025-23055 , CVE-2025-23056 , CVE-2025-23057)
Description	HPE has released security updates addressing multiple vulnerabilities in HPE Aruba Networking Fabric Composer. If exploited these vulnerabilities could cause privilege escalation, Authenticated Stored Cross-Site Scripting and unauthorized changes in critical system configurations HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking Fabric Composer 7.x.x: 7.1.0 and below
Officially Acknowledged by the Vendor	Yes
`Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04775en_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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public   Report incidents to incident@fincsirt.lk   TLP: WHITE