Advisory Alert

Alert Number:	AAA20250428	**Date:**	**April 28, 2025**	

Document Classification Level   **:**   Public Circulation Permitted | Public

Information Classification Level   **:**   TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SonicWall	**High**	Null Pointer Dereference Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security update addressing multiple vulnerabilities that exist in Dell PowerProtect Data Manager products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerProtect Data Manager Software Versions 19.15.0 through 19.18.0-23
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000311083/dsa-2025-062-security-update-for-dell-powerprotect-data-manager-multiple-security-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24813)
Description	IBM has released a security update addressing multiple vulnerabilities in Apache Tomcat that impact IBM QRadar SIEM. If exploited, these vulnerabilities could lead to Remote Code Execution, Information Disclosure, or Information Corruption. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP11 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7231915

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Null Pointer Dereference Vulnerability (CVE-2025-32818)
Description	SonicWall has released security updates addressing a Null Pointer Dereference vulnerability in their products. This vulnerability could be exploited by malicious users to compromise the affected system. **CVE-2025-32818** - A Null Pointer Dereference vulnerability in the SonicOS SSLVPN Virtual office interface allows a remote, unauthenticated attacker to crash the firewall, potentially leading to a Denial-of-Service (DoS) condition. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0009

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, 'The Zenith', 161A, Dharmapala Mawatha, Colombo 07, Sri Lanka
Hotline: + 94 112039777

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

Affected Product	Red Hat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2021-3690, CVE-2021-3859, CVE-2021-37714, CVE-2021-40690, CVE-2022-0084, CVE-2022-1319, CVE-2022-2053, CVE-2022-23913, CVE-2022-24785, CVE-2022-25647, CVE-2022-25857, CVE-2022-40149, CVE-2022-40152, CVE-2023-1108, CVE-2023-1973, CVE-2023-3223, CVE-2024-1635)
Description	Red Hat has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises applying the security fixes as soon as possible to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.1 EUS 7.1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:4226

Affected Product	IBM
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3690, CVE-2021-3859, CVE-2021-37714, CVE-2021-40690, CVE-2022-0084, CVE-2022-1319, CVE-2022-2053, CVE-2022-23913, CVE-2022-24785, CVE-2022-25647, CVE-2022-25857, CVE-2022-40149, CVE-2022-40152, CVE-2023-1108, CVE-2023-1973, CVE-2023-3223, CVE-2024-1635
Description	IBM has released a security update addressing multiple vulnerabilities in Apache Tomcat that impact IBM QRadar SIEM. If exploited, these vulnerabilities could lead to Out-of-bounds Write, Use After Free, Stack-based Buffer Overflow IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM 7.5 - 7.5.0 UP11 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7231915

Affected Product	Ubuntu
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7449-2

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, 'The Zenith', 161A, Dharmapala Mawatha, Colombo 07, Sri Lanka
Hotline: + 94 112039777

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