Advisory Alert

Alert Number: AAA20250507 **Date:** May 7, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
F5	**Medium**	Out-of-bounds Write Vulnerability
IBM	**Medium**	Multiple Denial of Service Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47535, CVE-2025-23367, CVE-2025-24970, CVE-2025-25193)
Description	Red Hat has released security updates addressing a multiple vulnerabilities that exist in JBoss Enterprise Application Platform. These vulnerabilities could be exploited by malicious users to cause Denial of Service, system crash and privilege escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:4552 • https://access.redhat.com/errata/RHSA-2025:4550 • https://access.redhat.com/errata/RHSA-2025:4549 • https://access.redhat.com/errata/RHSA-2025:4548

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52927, CVE-2023-52664, CVE-2024-26689, CVE-2024-56653, CVE-2025-21813)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. 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 24.10 Ubuntu 24.04 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7495-1 • https://ubuntu.com/security/notices/USN-7494-1 • https://ubuntu.com/security/notices/USN-7492-1 • https://ubuntu.com/security/notices/USN-7489-1

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Out-of-bounds Write Vulnerability (CVE-2024-36274)
Description	F5 has released security updates addressing an Out-of-bounds Write Vulnerability that exists in Intel Ethernet Controller and Adapter driver that affects rSeries appliances. **CVE-2024-36274** - Out-of-bounds write in the Intel(R) 800 Series Ethernet Driver for Intel(R) Ethernet Adapter Complete Driver Pack before versions 29.1 may allow an unauthenticated user to potentially enable denial of service via adjacent access. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A versions 1.8.0 and 1.5.1 - 1.5.3 running on all variants of the following rSeries appliances: r2000 series r4000 series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000151184

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2024-52903, CVE-2025-1493, CVE-2025-0915)
Description	IBM has released security updates addressing Multiple Denial of Service Vulnerabilities that exist in IBM Db2. **CVE-2024-52903** - IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query. **CVE-2025-1493** - IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to concurrent execution of shared resources. **CVE-2025-0915**- IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) under specific configurations could allow an authenticated user to cause a denial of service due to insufficient release of allocated memory resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 12.1.0 - 12.1.1 and 11.5.0 - 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7232336 • https://www.ibm.com/support/pages/node/7232518 • https://www.ibm.com/support/pages/node/7232529

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.