Advisory Alert

Alert Number:	AAA20241008	**Date:**	**October 8, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Security Update
IBM	**High** , **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-7885)
Description	Red Hat has released security updates addressing a flaw that could lead to information leakage in their products. **CVE-2024-7885 -** A vulnerability was found in Undertow where the ProxyProtocolReadListener reuses the same StringBuilder instance across multiple requests. This issue occurs when the parseProxyProtocolV1 method processes multiple requests on the same HTTP connection. As a result, different requests may share the same StringBuilder instance, potentially leading to information leakage between requests or responses. In some cases, a value from a previous request or response may be erroneously reused, which could lead to unintended data exposure. This issue primarily results in errors and connection termination but creates a risk of data leakage in multi-request environments. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:7736 • https://access.redhat.com/errata/RHSA-2024:7735

Affected Product	**IBM**
Severity	**High** , **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35195,CVE-2024-6345,CVE-2024-39689,CVE-2024-37891)
Description	IBM has released security patch updates addressing multiple vulnerabilities IBM Storage Protect Plus File Systems Agent. These vulnerabilities could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Plus File Systems Agent 10.1.6-10.1.16.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7172433

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