Advisory Alert

Alert Number: AAA20231103 **Date:** November 3, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Distributed Denial of Service Vulnerability
IBM	**High**, Medium	Multiple Vulnerabilities

Description

fected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Distributed Denial of Service Vulnerability (CVE-2023-44487)
Description	Redhat has released security updates addressing Distributed Denial of Service vulnerability within their products. The flaw due to incorrect handling of multiplexed streams in the HTTP/2 protocol. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat JBoss Data Grid Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:6286

Affected Product	**IBM**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-28327, CVE-2022-21680, CVE-2022-21681, CVE-2022-21702, CVE-2022-21703, CVE-2022-24675, CVE-2022-27664, CVE-2022-2879, CVE-2022-2880, CVE-2022-32189, CVE-2022-41715, CVE-2022-41721, CVE-2022-30633, CVE-2022-28131, CVE-2022-31107, CVE-2022-31097, CVE-2022-24785, CVE-2022-30629, CVE-2022-1650, CVE-2023-43804, CVE-2023-40217, CVE-2023-263690, CVE-2023-31484, CVE-2023-31486)
Description	IBM has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Privilege escalation, Cross-site scripting, Security restriction bypass, Sensitive information disclosure. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Storage Ceph prior to 6.1 IBM Storage Ceph 5.3z1-z4 IBM Spectrum Protect Plus File Systems Agent 10.1.6 - 10.1.14 IBM Storage Protect Plus File Systems Agent 10.1.15 AIX 7.2 AIX 7.3 VIOS 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7061952 https://www.ibm.com/support/pages/node/7061960 https://www.ibm.com/support/pages/node/7061948 https://www.ibm.com/support/pages/node/7061945 https://www.ibm.com/support/pages/node/7061939 https://www.ibm.com/support/pages/node/7061958 https://www.ibm.com/support/pages/node/7061953 https://www.ibm.com/support/pages/node/7061956 https://www.ibm.com/support/pages/node/7061966 https://www.ibm.com/support/pages/node/7061950 https://www.ibm.com/support/pages/node/7061949 https://www.ibm.com/support/pages/node/7061964 https://www.ibm.com/support/pages/node/7065539 https://www.ibm.com/support/pages/node/7047272

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.