Advisory Alert

Alert Number: AAA20230816 **Date:** August 16, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
IBM	**Medium**	Denial of service Vulnerability

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38401, CVE-2023-38402)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Privilege Escalation and Creation and Deletion of Arbitrary Files. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE Aruba Networking Virtual Intranet Access (VIA) client for Microsoft Windows:4.5.0 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04527en_us

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1055, CVE-2022-24963, CVE-2022-28331, CVE-2022-36760, CVE-2022-37436, CVE-2022-48279, CVE-2023-24021, CVE-2023-27522, CVE-2023-28319, CVE-2023-28321, CVE-2023-28322, CVE-2023-28484, CVE-2023-29469)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to HTTP response splitting, request smuggling, out-of-bounds write Red Hat recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64 Red Hat JBoss Core Services Text-Only Advisories x86_64 Red Hat Directory Server 11.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4629 https://access.redhat.com/errata/RHSA-2023:4628 https://access.redhat.com/errata/RHSA-2023:4655

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of service Vulnerability (CVE-2023-38737)
Description	IBM has released a security update addressing Denial of service Vulnerability that exist in IBM WebSphere Application Server Liberty. A remote attacker could exploit this vulnerability by sending a specially-Crafted request to WebSphere Application Server Liberty with the restfulWS-3.0 or restfulWS-3.1 feature enabled to cause to consume memory resources. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM WebSphere Application Server Liberty 22.0.0.13 - 23.0.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7027509

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.