Advisory Alert

Alert Number: AAA20230831 **Date:** August 31, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Access Bypass Vulnerability
HPE	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Privilege Escalation Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Access Bypass Vulnerability (CVE-2022-1996)
Description	IBM has released a security update addressing an Access Bypass Vulnerability that exist in their products. **CVE-2022-1996** - The vulnerability allows a remote attacker to bypass the CORS protection mechanism. The vulnerability exists due to incorrect processing of the "Origin" HTTP header that is supplied within HTTP request. A remote attacker can supply arbitrary value via the "Origin" HTTP header, bypass implemented CORS protection mechanism and perform cross-site scripting attacks against the vulnerable application. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Storage Defender - Data Protect 1.0.0 - 1.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7029861

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39266, CVE-2023-39267, CVE-2023-39268)
Description	HPE has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities could lead to Denial of Service (DoS), Disclosure of Sensitive Information, Memory corruption. HPE recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Aruba 5400R Series Switches Aruba 3810 Series Switches Aruba 2920 Series Switches Aruba 2930F Series Switches Aruba 2930M Series Switches Aruba 2530 Series Switches Aruba 2540 Series Switches
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04533en_us

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-42896, CVE-2023-1829, CVE-2023-3390, CVE-2023-35788, CVE-2023-3090, CVE-2023-2124, CVE-2022-1353, CVE-2022-39188, CVE-2023-0458, CVE-2023-28466, CVE-2021-33656, CVE-2023-1637, CVE-2023-2002, CVE-2023-20593)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities could lead to Out-of-bounds write, Race condition, Sensitive information disclosure, Arbitrary read and write. Redhat recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4888 https://access.redhat.com/errata/RHSA-2023:4834 https://access.redhat.com/errata/RHSA-2023:4829 https://access.redhat.com/errata/RHSA-2023:4817 https://access.redhat.com/errata/RHSA-2023:4801 https://access.redhat.com/errata/RHSA-2023:4789

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-17142, CVE-2018-17847, CVE-2018-17848, CVE-2020-14040, CVE-2020-8203, CVE-2020-9283, CVE-2021-23337, CVE-2021-23341, CVE-2021-3801, CVE-2022-31129, CVE-2023-20867, CVE-2023-30861, CVE-2023-24329, CVE-2023-32067, CVE-2022-48339, CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, CVE-2023-21968, CVE-2022-1996, CVE-2014-3566, CVE-2022-3064, CVE-2021-4235, CVE-2019-11254, CVE-2022-32149, CVE-2021-27116, CVE-2021-27117, CVE-2022-41721, CVE-2022-41723, CVE-2021-23440, CVE-2018-25031, CVE-2022-46175, CVE-2022-37599, CVE-2022-37603, CVE-2023-29401, CVE-2022-25881, CVE-2023-2251)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities could lead to Information disclosure, Denial of service, Arbitrary command execution, Privilege escalation. IBM recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM Storage Defender - Data Protect 1.0.0 - 1.2.0 IBM System Storage Tape Controller 3592 Model C07 IBM Storage Fusion 2.1.0 - 2.4.0 IBM Storage Fusion HCI 2.1.0 - 2.4.1 IBM Spectrum Fusion 2.1.0 - 2.5.2 IBM Spectrum Fusion HCI 2.1.0 - 2.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7029861 https://www.ibm.com/support/pages/node/690117 https://www.ibm.com/support/pages/node/7029668 https://www.ibm.com/support/pages/node/7029670 https://www.ibm.com/support/pages/node/7029669

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4015, CVE-2023-3777, CVE-2023-3611, CVE-2023-20593, CVE-2022-40982, CVE-2023-3776, CVE-2023-4004, CVE-2023-3609, CVE-2023-3995, CVE-2023-3610, CVE-2023-21400, CVE-2022-0168, CVE-2022-1184, CVE-2023-3141, CVE-2022-27672, CVE-2020-36691, CVE-2022-4269, CVE-2023-2124, CVE-2023-30772, CVE-2023-28466, CVE-2023-0590, CVE-2023-2194, CVE-2023-33203, CVE-2023-1611, CVE-2023-1990, CVE-2023-3111, CVE-2023-1855)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of these vulnerabilities could lead to Sensitive information disclosure, Denial of service and Arbitrary code execution Ubuntu recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 23.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6321-1 https://ubuntu.com/security/notices/USN-6318-1 https://ubuntu.com/security/notices/USN-6317-1 https://ubuntu.com/security/notices/USN-6316-1 https://ubuntu.com/security/notices/USN-6315-1 https://ubuntu.com/security/notices/USN-6314-1

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-20266)
Description	Cisco has released security updates addressing a Privilege Escalation Vulnerability that exist in their products. **CVE-2023-20266** - A vulnerability in Cisco Emergency Responder, Cisco Unified Communications Manager (Unified CM), Cisco Unified Communications Manager Session Management Edition (Unified CM SME), and Cisco Unity Connection could allow an authenticated, remote attacker to elevate privileges to root on an affected device. This vulnerability exists because the application does not properly restrict the files that are being used for upgrades Cisco recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Cisco Emergency Responder Cisco Unified CM Cisco Unified CM SME Cisco Unity Connection
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-priv-esc-D8Bky5eg

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.