Advisory Alert

Alert Number: AAA20240131 **Date:** January 31, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Denial Of Service Vulnerability
IBM	**High**	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20253, CVE-2024-20272)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their product. **CVE-2024-20253** - A Remote Code Execution Vulnerability exists within multiple Cisco Unified Communications and Contact Center Solutions products. An attacker could exploit this vulnerability by sending a crafted message to the listening port of an affected device, which could lead to the execution of arbitrary commands on the underlying operating system with the privileges of the web services user. **CVE-2024-20272** - An Unauthenticated Arbitrary File Upload Vulnerability exists within the web-based management interface of the Cisco Unity Connection. An unauthenticated remote attacker could upload arbitrary files to an affected system, execute commands on the underlying operating system, and elevate privileges to root. This vulnerability is due to a lack of authentication in a specific API and improper validation of user-supplied data. It is strongly recommended to apply the necessary remediation at your earliest to avoid issues. We have already addressed these vulnerabilities in the **AAA20240126** Advisory alert before.
Affected Products	Unified Communications Manager (Unified CM) (CSCwd64245) Unified Communications Manager IM & Presence Service (Unified CM IM&P) (CSCwd64276) Unified Communications Manager Session Management Edition (Unified CM SME) (CSCwd64245) Unified Contact Center Express (UCCX) (CSCwe18773) Unity Connection (CSCwd64292) Virtualized Voice Browser (VVB) (CSCwe18840) 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-rce-bWNzQcUm https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2021-4048)
Description	IBM has released a security updates addressing a Denial Of Service vulnerability that exist in Netlib LAPACK library of QRadar SIEM. The vulnerability is caused due to an out-of-bounds read flaw in the CLARRV, DLARRV, SLARRV, and ZLARRV functions. By sending specially-crafted inputs, a remote attacker could exploit this vulnerability to cause the application to crash or obtain portions of memory information. IBM strongly recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	IBM QRadar User Behavior Analytics 1.0.0 - 4.1.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7112498

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31484, CVE-2023-1370, CVE-2021-23445, CVE-2021-31684)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in QRadar SIEM. If exploited by an attacker it could lead to man-in-the-middle attack, cross-site scripting, and denial of service. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	IBM QRadar User Behavior Analytics 1.0.0 - 4.1.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7112498

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0458, CVE-2023-1073, CVE-2023-1075, CVE-2023-1079, CVE-2023-1838, CVE-2023-1855, CVE-2023-2162, CVE-2023-2163, CVE-2023-3141, CVE-2023-3567, CVE-2023-3611, CVE-2023-3772, CVE-2023-3812, CVE-2023-4132, CVE-2023-4622, CVE-2023-4623, CVE-2023-5178, CVE-2023-5717, CVE-2023-23455, CVE-2023-26545, CVE-2023-28328, CVE-2023-31436, CVE-2023-33203, CVE-2023-35823, CVE-2023-35824, CVE-2023-35825, CVE-2023-45871, CVE-2023-46813, CVE-2021-3750, CVE-2023-3019, CVE-2023-2163, CVE-2023-3812, CVE-2023-4622, CVE-2023-4623, CVE-2023-4921, CVE-2023-42753, CVE-2023-45871)
Description	Red Hat has released security updates addressing Multiple Vulnerabilities that exist in their products. An attacker could exploit these vulnerabilities to cause Use after free condition, Race Condition, Bugs for oversize packets, potential slab-out-of-bound access. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 8.8 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0575 https://access.redhat.com/errata/RHSA-2024:0569 https://access.redhat.com/errata/RHSA-2024:0593

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.