Advisory Alert

Alert Number: AAA20240206 **Date:** February 6, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Unauthenticated Arbitrary File Upload Vulnerability
Suse	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Arbitrary File Upload Vulnerability (CVE-2024-20272)
Description	Cisco has released a security update addressing an Unauthenticated arbitrary file upload vulnerability that exists in Cisco Unity Connection. A successful exploit could allow the attacker to store malicious files on the system, execute arbitrary commands on the operating system, and elevate privileges to root. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Unity Connection Release 14, 12.5 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5178, CVE-2023-6176, CVE-2023-6932)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. An attacker could exploit these vulnerabilities to cause Denial of service and User after free condition. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240331-1 https://www.suse.com/support/update/announcement/2024/suse-su-20240339-1 https://www.suse.com/support/update/announcement/2024/suse-su-20240344-1

Affected Product	**IBM**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46308, CVE-2023-32006, CVE-2023-32002, CVE-2022-25883, CVE-2023-32559)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in the IBM QRadar Pulse App. An attacker could exploit these vulnerabilities to cause Security restriction bypass, Denial of service and Arbitrary code execution IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar Pulse App 1.0.0 - 2.2.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7114777

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.