Advisory Alert

Alert Number: **AAA20230228** **Date:** **February 28, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1629, CVE-2022-1621, CVE-2022-1897, CVE-2022-1785, CVE-2022-1927, CVE-2022-27774, CVE-2022-22576, CVE-2022-27776, CVE-2022-27775, CVE-2022-29824, CVE-2022-1586, CVE-2022-25314, CVE-2021-40528)
Description	IBM has released Security Updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause buffer overflow, execute arbitrary code, sensitive information disclosure, bypass access authentication, obtain authentication, cookie header data information disclosure, denial of service. IBM recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	IBM QRadar SIEM 7.4.0 - 7.4.3 Fix Pack 7 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Pack 3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6958506

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3564, CVE-2023-0179)
Description	SUSE has released security updates to address multiple vulnerabilities that exist in their products and, packagers that used by their products. These vulnerabilities allow an attacker to compromise vulnerable systems. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP1, SP2, SP3 SUSE Linux Enterprise Live Patching 12-SP4 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15- SP1, SP2, SP3 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Server 12 SP4 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server for SAP Applications 12 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP1, SP2, SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230519-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230523-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230522-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230525-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230528-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230547-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230552-1/

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.