TLP: WHITE

Advisory Alert

Alert Number: **AAA20240506** **Date:** **May 6, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
SolarWinds	**Medium**	Arbitrary File Overwrite Vulnerability

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45871, CVE-2023-42282)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in IBM Storage Scale products. **CVE-2023-45871** - By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code or cause a denial of service condition on the system. **CVE-2023-42282** - By sending a specially crafted request using a hexadecimal representation of a private IP address, an attacker could exploit this vulnerability to execute arbitrary code on the system and obtain sensitive information. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Scale versions 5.1.0.0 - 5.1.9.2 IBM Storage Scale System versions 6.1.0.0 - 6.1.2.8 and 6.1.3.0 - 6.1.9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7150143 • https://www.ibm.com/support/pages/node/7150147

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-1086, CVE-2023-6546)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Linux kernel. **CVE-2024-1086** - A flaw was found in the Netfilter subsystem in the Linux kernel. This issue occurs in the nft_verdict_init() function, allowing positive values as a drop error within the hook verdict, therefore, the nf_hook_slow() function can cause a double-free vulnerability when NF_DROP is issued with a drop error that resembles NF_ACCEPT. The nf_tables component can be exploited to achieve local privilege escalation. **CVE-2023-6546** - A race condition was found in the GSM 0710 tty multiplexor in the Linux kernel. This issue occurs when two threads execute the GSMIOC_SETCONF ioctl on the same tty file descriptor with the gsm line discipline enabled, and can lead to a use-after-free problem on a struct gsm_dlci while restarting the gsm mux. This could allow a local unprivileged user to escalate their privileges on the system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:2697

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Use-After-Free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5, 15.3 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP5, 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Server 15 SP5, 15 SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241490-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241489-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2015-3627, CVE-2018-20060, CVE-2019-11236, CVE-2019-11324, CVE-2019-9740, CVE-2020-26137, CVE-2021-30465, CVE-2021-33503, CVE-2021-43565, CVE-2021-43784, CVE-2022-29162, CVE-2012-2677, CVE-2023-1192, CVE-2023-22067, CVE-2023-22081, CVE-2023-25809, CVE-2023-26159, CVE-2023-27561, CVE-2023-27859, CVE-2023-28642, CVE-2023-28840, CVE-2023-28841, CVE-2023-28842, CVE-2023-29483, CVE-2023-3609, CVE-2023-38325, CVE-2023-38729, CVE-2023-42282, CVE-2023-43804, CVE-2023-44270, CVE-2023-45193, CVE-2023-45803, CVE-2023-45857, CVE-2023-45871, CVE-2023-46136, CVE-2023-47141, CVE-2023-47145, CVE-2023-47152, CVE-2023-47158, CVE-2023-4732, CVE-2023-47746, CVE-2023-47747, CVE-2023-50308, CVE-2023-50782, CVE-2023-5178, CVE-2023-52296, CVE-2023-5676, CVE-2023-6681, CVE-2024-1135, CVE-2024-21501, CVE-2024-21503, CVE-2024-22195, CVE-2024-22360, CVE-2024-24758, CVE-2024-25030, CVE-2024-25046, CVE-2024-26130, CVE-2024-27088, CVE-2024-27254, CVE-2024-28102)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Sensitive Information Disclosure, Arbitrary Code Execution, Cross-Site Scripting. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QRadar Suite Software versions 1.10.12.0 - 1.10.20.0 IBM SOAR QRadar Plugin App versions 1.0 - 5.3.1 IBM® Db2® versions 10.5.0.x 11.1.4.x 11.5.x IBM Storage Scale System versions 6.1.0.0 - 6.1.2.8 and 6.1.3.0 - 6.1.9.1 IBM Storage Scale versions 5.1.0.0 - 5.1.9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7150150 • https://www.ibm.com/support/pages/node/7150196 • https://www.ibm.com/support/pages/node/7150158 • https://www.ibm.com/support/pages/node/7150144 • https://www.ibm.com/support/pages/node/7150143 • https://www.ibm.com/support/pages/node/7150147

Affected Product	**SolarWinds**
Severity	**Medium**
Affected Vulnerability	Arbitrary File Overwrite Vulnerability (CVE-2024-28072)
Description	SolarWinds has released security updates addressing an Arbitrary File Overwrite Vulnerability that exists in Serv-U that allows a highly privileged account to overwrite arbitrary files on the system with log output. The log file path tags were not sanitized properly. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Serv-U 15.4.2 and previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28072

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.