Advisory Alert

Alert Number: **AAA20230425** **Date:** **April 25, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
SolarWinds	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2991, CVE-2023-0590, CVE-2023-1118)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. **CVE-2022-2991** - A heap-based buffer overflow exists due to improper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. This vulnerability allows a local attacker with the ability to execute high-privileged code on the target system to escalate privileges and execute arbitrary code in the context of the kernel. **CVE-2023-0590**- A use-after-free flaw was found in qdisc_graft in net/sched/sch_api.c in the Linux Kernel due to a race problem. This flaw leads to a denial of service issue. If patch ebda44da44f6 ("net: sched: fix race condition in qdisc_graft()") not applied yet, then kernel could be affected. **CVE-2023-1118**- Linux kernel integrated infrared receiver/transceiver driver contains a use after free flaw in the way user detaching rc device. A local user could use this flaw to crash the system or potentially escalate their privileges on the system. Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP4 SUSE Linux Enterprise Live Patching 12-SP4 SUSE Linux Enterprise Server 12 SP4 SUSE Linux Enterprise Server for SAP Applications 12 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20231971-1/

Affected Product	**SolarWinds**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36963, CVE-2022-47509, CVE-2022-47505)
Description	SolarWinds has released security updates addressing multiple vulnerabilities affecting SolarWinds Platform. **CVE-2022-36963** - The SolarWinds Platform contains a Command Injection vulnerability that allows a remote adversary with a valid SolarWinds Platform admin account to execute arbitrary commands. **CVE-2022-47509** - A Neutralization vulnerability exists in SolarWinds Platform that allows a remote adversary with a valid SolarWinds Platform account to append URL parameters to inject HTML. **CVE-2022-47505** - A Local Privilege Escalation vulnerability exists in SolarWinds Platform that allows a local adversary with a valid system user account to escalate local privileges. SolarWinds recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	SolarWinds Platform 2023.1 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2022-47505 https://www.solarwinds.com/trust-center/security-advisories/cve-2022-47509 https://www.solarwinds.com/trust-center/security-advisories/cve-2022-36963

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-30456, CVE-2023-28866, CVE-2023-28466, CVE-2023-28328, CVE-2023-26607, CVE-2023-26605, CVE-2023-26545, CVE-2023-25012, CVE-2023-23559, CVE-2023-23455, CVE-2023-1998, CVE-2023-1990, CVE-2023-1989, CVE-2023-1855, CVE-2023-1829, CVE-2023-1670, CVE-2023-1583, CVE-2023-1281, CVE-2023-1118, CVE-2023-1095, CVE-2023-1079, CVE-2023-1077, CVE-2023-1076, CVE-2023-1074, CVE-2023-1073, CVE-2023-1032, CVE-2023-0394, CVE-2023-0266, CVE-2023-0045, CVE-2022-47929, CVE-2022-4382, CVE-2022-4269, CVE-2022-41849, CVE-2022-4129, CVE-2022-41218, CVE-2022-3903, CVE-2022-36280, CVE-2022-3424, CVE-2022-3108, CVE-2022-21505, CVE-2021-3669)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, Sensitive information disclosure, Arbitrary code execution and Kernel lockdown restrictions Bypass. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 18.04 Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6027-1 https://ubuntu.com/security/notices/USN-6029-1 https://ubuntu.com/security/notices/USN-6030-1 https://ubuntu.com/security/notices/USN-6031-1 https://ubuntu.com/security/notices/USN-6032-1 https://ubuntu.com/security/notices/USN-6033-1

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.