Advisory Alert

Alert Number: AAA20230301 **Date:** March 1, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
HP	**High**, Medium	Multiple Vulnerabilities
Dell	Medium	Improper Authorization vulnerability
Ubuntu	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2873, CVE-2022-3564, CVE-2022-4378, CVE-2022-4379, CVE-2023-0179)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-2873** - Linux kernel Intel's iSMT SMBus host controller driver contains an out-of-bounds memory access flaw in the way a user triggers the I2C_SMBUS_BLOCK_DATA (with the ioctl I2C_SMBUS) with malicious input data. This flaw allows a local user to crash the system. **CVE-2022-3564** - Linux kernel's L2CAP bluetooth functionality contains a use-after-free flaw which is exploited when a user triggers a race condition by two malicious flows in the L2CAP bluetooth packets. This flaw allows a local or bluetooth connection user to crash the system or potentially escalate privileges. **CVE-2022-4378** - Linux kernel's SYSCTL subsystem contains a stack overflow flaw that can be triggered when a user changes certain kernel parameters and variables. This flaw allows a local user to crash or potentially escalate their privileges on the system. **CVE-2022-4379** - A use-after-free vulnerability was found in __nfs42_ssc_open() in fs/nfs/nfs4file.c in the Linux kernel. This flaw allows an attacker to conduct a remote denial of service. **CVE-2023-0179** - Linux Kernel Netfilter subsystem contains a buffer overflow vulnerability. This issue could allow the leakage of both stack and heap addresses, and potentially allow Local Privilege Escalation to the root user via arbitrary code execution. Redhat recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64, NFV 9 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.7 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64, TUS 7.7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:0979 https://access.redhat.com/errata/RHSA-2023:1008 https://access.redhat.com/errata/RHSA-2023:0945 https://access.redhat.com/errata/RHSA-2023:0944

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3564, CVE-2022-42826, CVE-2022-42852, CVE-2022-42863, CVE-2022-42867, CVE-2022-45063, CVE-2022-46691, CVE-2022-46692, CVE-2022-46698, CVE-2022-46699, CVE-2022-46700, CVE-2023-0179, CVE-2023-23517, CVE-2023-23518, CVE-2023-23529)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to command injection, arbitrary command injection, sensitive information disclosure, Same Origin Policy bypass. Suse recommends to apply necessary fixes to avoid issues.
Affected Products	SUSE CaaS Platform 4.0 SUSE Enterprise Storage 6 SUSE Linux Enterprise High Performance Computing 12 SP2, SP4, SP5 SUSE Linux Enterprise High Performance Computing 15 SP1, SP1 LTSS 15-SP1, SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Server 12 SP2, SP2 BCL 12-SP2, SP4, SP4 ESPOS 12-SP4, SP4 LTSS 12-SP4, 12 SP5 SUSE Linux Enterprise Server 15 SP1, SP1 LTSS 15-SP1, SP3 SUSE Linux Enterprise Server for SAP Applications 12 SP4, SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP1, SP3 SUSE OpenStack Cloud 9, Cloud Crowbar 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230582-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230578-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230573-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-38712, 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 vulnerability that exist in WebSphere Application Server and QRadar SIEM Application Framework. Exploitation of these vulnerabilities could lead to arbitrary code execution, access bypass, sensitive information disclosure, SOAPAction spoofing IBM recommends to apply necessary fixes to avoid issues.
Affected Products	Websphere Application Server 9.0, 8.5, 8.0 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/6958478 https://www.ibm.com/support/pages/node/6958506

Affected Product	**HP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3712, CVE-2023-22747, CVE-2023-22748, CVE-2023-22749, CVE-2023-22750, CVE-2023-22751, CVE-2023-22752, CVE-2023-22753, CVE-2023-22754, CVE-2023-22755, CVE-2023-22756, CVE-2023-22757, CVE-2023-22758, CVE-2023-22759, CVE-2023-22760, CVE-2023-22761, CVE-2023-22762, CVE-2023-22763, CVE-2023-22764, CVE-2023-22765, CVE-2023-22766, CVE-2023-22767, CVE-2023-22768, CVE-2023-22769, CVE-2023-22770, CVE-2023-22771, CVE-2023-22772, CVE-2023-22773, CVE-2023-22774, CVE-2023-22775, CVE-2023-22776, CVE-2023-22777, CVE-2023-22778, CVE-2022-21216)
Description	HP has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to privilege escalation, Cross-Site Scripting (XSS); Remote: Arbitrary Code Execution, Arbitrary Command Execution, Arbitrary File Deletion, Disclosure of Sensitive Information, Unauthorized Arbitrary Command Execution, Buffer Overflow, Session Reuse HP recommends to apply necessary fixes to avoid issues.
Affected Products	HPE Edgeline e920 Server Blade -Prior to 1.66_02-02-2023 HPE Edgeline e920d Server Blade -Prior to 1.66_02-02-2023 HPE Edgeline e920t Server Blade -Prior to 1.66_02-02-2023 ArubaOS 8.6.x.x: 8.6.0.19 and below ArubaOS 8.10.x.x: 8.10.0.4 and below ArubaOS 10.3.x.x: 10.3.1.0 and below SD-WAN 8.7.0.0-2.3.0.x: 8.7.0.0-2.3.0.8 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04410en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04454en_us

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Improper Authorization vulnerability (CVE-2022-46752)
Description	Dell has released a Security Update addressing an Improper Authorization vulnerability that exist in their products. An unauthenticated physical attacker can exploit this vulnerability to cause denial of service. Dell recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Inspiron 14 Plus 7420, 16 Plus 7620, 3511, 3511, 3520, 5310, 5320, 5410, 5410, 5420, 5510, 5620, 7420, 7510, 7610, 7620 Latitude 3140, 3320, 3420, 3430, 3520, 3530, 5330, 5420, 5430, 5430 Rugged, 5431, 5520, 5521, 5530, 5531, 7320, 7320 Detachable, 7330, 7420, 7430, 7520, 7530, 9330, 9420, 9430, 9510, 9520, Rugged 7330 Precision 3470, 3560, 3561, 3570, 3571, 5470, 5560, 5570, 5760, 5770, 7560, 7670, 7760, 7770 Vostro 3420, 3510, 3510, 3520, 5310, 5320, 5410, 5510, 5620, 7510, 7620 XPS 13 9315, 13 9315 2-in-1, 13 9320, 15 9510, 15 9520, 17 9710, 17 9720
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000207928/dsa-2023-011

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41556, CVE-2022-22707, CVE-2023-0568, CVE-2023-0567, CVE-2023-0662, CVE-2023-0361, CVE-2023-21830, CVE-2023-21843, CVE-2023-21835)
Description	Ubuntu has released Security Updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to denial of service, sensitive information disclosure, restriction bypass. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 22.10 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5903-1 https://ubuntu.com/security/notices/USN-5902-1 https://ubuntu.com/security/notices/USN-5901-1 https://ubuntu.com/security/notices/USN-5898-1 https://ubuntu.com/security/notices/USN-5897-1

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.