Advisory Alert

Alert Number: AAA20230823 **Date:** August 23, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
IBM	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40982, CVE-2023-0459, CVE-2023-20569, CVE-2023-21400, CVE-2023-2156, CVE-2023-2166, CVE-2023-31083, CVE-2023-3268, CVE-2023-3567, CVE-2023-3609, CVE-2023-3611, CVE-2023-3776, CVE-2023-38409, CVE-2023-3863, CVE-2023-4004)
Description	Suse has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the vulnerabilities could lead to side channel attack, memory access flaw, memory corruption, race condition. Suse recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	openSUSE Leap 15.4, 15.5 Public Cloud Module 15-SP4, 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233376-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233377-1

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20593, CVE-2023-32233, CVE-2023-35788)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2023-20593** - A flaw was found in hw, in “Zen 2” CPUs. This issue may allow an attacker to access sensitive information under specific microarchitectural circumstances. **CVE-2023-32233** - A use-after-free vulnerability was found in the Netfilter subsystem of the Linux kernel when processing batch requests to update nf_tables configuration. This vulnerability can be abused to perform arbitrary reads and writes in kernel memory. **CVE-2023-35788** - A flaw was found in the TC flower classifier (cls_flower) in the Networking subsystem of the Linux kernel. This issue occurs when sending two TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets with a total size of 252 bytes, which results in an out-of-bounds write when the third packet enters fl_set_geneve_opt, potentially leading to a denial of service or privilege escalation. Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux Server - TUS 7.7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.7 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.7 x86_64 Red Hat Enterprise Linux Server - AUS 7.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4699 https://access.redhat.com/errata/RHSA-2023:4697 https://access.redhat.com/errata/RHSA-2023:4696

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-33894, CVE-2022-38087)
Description	Dell has released security updates addressing multiple vulnerabilities that exists in third party components that in turn affect Dell products. **CVE-2022-33894** - Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access. **CVE-2022-38087** - Exposure of resource to wrong sphere in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access. Dell recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000213216/dsa-2023-096-security-update-for-dell-poweredge-server-for-intel-may-2023-security-advisories-2023-2-ipu

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-37421, CVE-2023-37422, CVE-2023-37423, CVE-2023-37424, CVE-2023-37425, CVE-2023-37426, CVE-2023-37427, CVE-2023-37428, CVE-2023-37429, CVE-2023-37430, CVE-2023-37431, CVE-2023-37432, CVE-2023-37433, CVE-2023-37434, CVE-2023-37435, CVE-2023-37436, CVE-2023-37437, CVE-2023-37438, CVE-2023-37439, CVE-2023-37440)
Description	HPE has released security updates addressing multiple vulnerabilities that exists in HPE Aruba EdgeConnect SD-WAN products. Successful exploitation of the vulnerabilities could lead to Arbitrary Code Execution, Cross-Site Scripting (XSS), Disclosure of Sensitive Information, SQL Injection, and Server-Side Request Forgery (SSRF). HPE recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	EdgeConnect SD-WAN Orchestrator (self-hosted, on-premises) EdgeConnect SD-WAN Orchestrator (self-hosted, public cloud IaaS) EdgeConnect SD-WAN Orchestrator-as-a-Service EdgeConnect SD-WAN Orchestrator-SP Tenant Orchestrators EdgeConnect SD-WAN Orchestrator Global Enterprise Tenant Orchestrators. • Orchestrator 9.3.x: Orchestrator 9.3.0 (all builds) and below • Orchestrator 9.2.x: Orchestrator 9.2.5 (all builds) and below • Orchestrator 9.1.x: Orchestrator 9.1.7 (all builds) and below • Orchestrator 9.0.x: All versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04531en_us

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22045, CVE-2023-22049, CVE-2020-4329)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2023-22045** - An unspecified vulnerability in Java SE related to the VM component could allow a remote attacker to cause low confidentiality impacts. **CVE-2023-22049** - An unspecified vulnerability in Java SE related to the Libraries component could allow a remote attacker to cause low integrity impacts. **CVE-2020-4329** - IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0, 8.5 IBM WebSphere Application Server Liberty Continuous delivery InfoSphere Master Data Management 11.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7028350 https://www.ibm.com/support/pages/node/7028226

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.