Advisory Alert

Alert Number: **AAA20240228** **Date:** **February 28, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Suse	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
F5	**High**	Use-after-free Vulnerability
VMware	**Medium**	Out-of-bounds read Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE: CVE-2024-26294, CVE-2024-26295, CVE-2024-26296, CVE-2024-26297, CVE-2024-26298, CVE-2024-26299, CVE-2024-26300, CVE-2024-26301, CVE-2024-26302, CVE-2023-50164)
Description	HPE has released a security update addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Remote: Arbitrary Code Execution, Code Execution, Cross-Site Scripting (XSS), Disclosure of Sensitive Information HPE strongly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE Aruba ClearPass Policy Manager 6.12.x: 6.12.0 HPE Aruba ClearPass Policy Manager 6.11.x: 6.11.6 and below HPE Aruba ClearPass Policy Manager 6.10.x: ClearPass 6.10.8 Hotfix Q4 2023 for Security issues and below HPE Aruba ClearPass Policy Manager 6.9.x: ClearPass 6.9.13 Hotfix Q4 2023 for Security issues and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04601en_us

Affected Product	**Suse**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-30187, CVE-2021-42740, CVE-2022-0860, CVE-2022-1415, CVE-2022-31129, CVE-2022-40152)
Description	Suse has released a security update addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Information disclosure and Deserialization of Untrusted Data. Suse strongly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4, 15.5 Public Cloud Module 15-SP1, 15-SP2, 15-SP3, 15-SP4, 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5 SUSE Manager Proxy 4.0, 4.1, 4.3 SUSE Manager Proxy 4.2 Module 4.2 SUSE Manager Retail Branch Server 4.0, 4.1, 4.2, 4.3 SUSE Manager Server 4.0, 4.1, 4.2, 4.3 SUSE Manager Server 4.2 Module 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232897-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20230592-1/

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3523, CVE-2022-36280, CVE-2023-0045, CVE-2023-0122, CVE-2023-0461, CVE-2023-0590, CVE-2023-0597, CVE-2023-1118, CVE-2023-22995, CVE-2023-22998, CVE-2023-23000, CVE-2023-23004, CVE-2023-23454, CVE-2023-23455, CVE-2023-23559, CVE-2023-26545, CVE-2020-8908, CVE-2022-0860, CVE-2023-22644, CVE-2022-46146, CVE-2022-2196, CVE-2022-4269, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2022-4744, CVE-2023-0179, CVE-2023-0394, CVE-2023-0469, CVE-2023-1075, CVE-2023-1076, CVE-2023-1077, CVE-2023-1079, CVE-2023-1095, CVE-2023-1380, CVE-2023-1382, CVE-2023-1513, CVE-2023-1582, CVE-2023-1583, CVE-2023-1611, CVE-2023-1637, CVE-2023-1652, CVE-2023-1670, CVE-2023-1838, CVE-2023-1855, CVE-2023-1989, CVE-2023-1998, CVE-2023-2002, CVE-2023-21102, CVE-2023-21106, CVE-2023-2124, CVE-2023-2156, CVE-2023-2162, CVE-2023-2176, CVE-2023-2235, CVE-2023-2269, CVE-2023-23001, CVE-2023-23006, CVE-2023-2483, CVE-2023-25012, CVE-2023-2513, CVE-2023-28327, CVE-2023-28410, CVE-2023-28464, CVE-2023-3006, CVE-2023-30456, CVE-2023-30772, CVE-2023-31084, CVE-2023-3141, CVE-2023-31436, CVE-2023-3161, CVE-2023-32233, CVE-2023-33288, CVE-2023-33951, CVE-2023-33952, CVE-2023-51780)
Description	Suse has released a security update addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Out-of-bounds memory access, Null pointer deference, Race condition, Denial of service, Integer overflow. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Development Tools Module 15-SP4 openSUSE Leap 15.3, 15.4, 15.5 Public Cloud Module 15-SP4, 15-SP5 SUSE Enterprise Storage 7, 7.1 SUSE Linux Enterprise Desktop 15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise High Performance Computing 15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server 15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15, 15 SP1, 15 SP2, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Manager Client Tools for SLE 15 SUSE Manager Proxy 4.2, 4.3 SUSE Manager Retail Branch Server 4.2, 4.3 SUSE Manager Server 4.2, 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230774-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231831-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232181-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232594-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232646-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240639-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3609, CVE-2023-4921, CVE-2023-42753, CVE-2023-45871)
Description	Red Hat has released a security update addressing multiple vulnerabilities. **CVE-2023-3609** - A double-free flaw was found in u32_set_parms in net/sched/cls_u32.c in the Network Scheduler component in the Linux kernel. This flaw allows a local attacker to use a failure event to mishandle the reference counter, leading to a local privilege escalation threat. **CVE-2023-4921** - A use-after-free flaw was found in qfq_dequeue and agg_dequeue in net/sched/sch_qfq.c in the Traffic Control (QoS) subsystem in the Linux kernel. This issue may allow a local user to crash the system or escalate their privileges on the system. **CVE-2023-42753** - An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the h->nets array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. **CVE-2023-45871** - A flaw was found in igb_configure_rx_ring in drivers/net/ethernet/intel/igb/igb_main.c in the IGB driver in the Linux kernel. An overflow of the contents from a packet that is too large will overflow into the kernel's ring buffer, leading to a system integrity issue. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0999

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20952, CVE-2023-33850)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in IBM Java SDK and IBM Java Runtime that affect IBM Db2. **CVE-2024-20952** - An unspecified vulnerability in Java SE related to the Security component could allow a remote attacker to cause high confidentiality impact and high integrity impact. **CVE-2023-33850**- IBM GSKit-Crypto could allow a remote attacker to obtain sensitive information, caused by a timing-based side channel in the RSA Decryption implementation. By sending an overly large number of trial messages for decryption, an attacker could exploit this vulnerability to obtain sensitive information. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Db2 10.5.0.x Client and Server IBM Db2 11.1.4.x Client and Server IBM Db2 11.5.x Client and Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7124105

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2023-3776)
Description	F5 has released a security update addressing a use-after-free vulnerability that exist in their products. The vulnerability exist in the Linux kernel's net/sched: cls_fw component which could be exploited to achieve local privilege escalation. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Traffix SDC 5.2.0, 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138731

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Out-of-bounds read Vulnerability (CVE-2024-22251)
Description	VMware has released a security update addressing an Out-of-bounds read vulnerability that exist in VMware Workstation and Fusion’s USB CCID (chip card interface device). A malicious actor with local administrative privileges on a virtual machine may trigger an out-of-bounds read leading to information disclosure. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Workstation 17.x Fusion 13.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2024-0005.html

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.