Advisory Alert

Alert Number: AAA20240327 **Date:** March 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Arbitrary Code Execution Vulnerability
HPE	**High**	Multiple Denial of Service Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
WatchGuard	**High**	Local Code Injection Vulnerability
IBM	**High**, Medium	Multiple Vulnerabilities
Oracle	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium, Low	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35116, CVE-2023-34453, CVE-2023-34455, CVE-2023-34454, CVE-2023-43642, CVE-2023-2976, CVE-2023-33201, CVE-2023-46136, CVE-2023-43804, CVE-2023-37920, CVE-2022-25883, CVE-2023-45133, CVE-2023-31484, CVE-2023-1370, CVE-2021-4048, CVE-2021-23445, CVE-2021-31684, CVE-2023-38019, CVE-2023-38020, CVE-2023-38263, CVE-2023-46308, CVE-2023-32006, CVE-2023-32002, CVE-2023-32559, CVE-2022-38900, CVE-2023-45857, CVE-2022-25927, CVE-2023-44270, CVE-2023-26159, CVE-2020-19909, CVE-2023-0727, CVE-2023-6129, CVE-2023-5363, CVE-2022-21216)
Description	Juniper has issued security updates addressing multiple vulnerabilities that exist in JSA Applications. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Denial of Service, Cross-Site Scripting, Information Disclosure, Privilege Escalation, SQL Injection. Juniper advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Log Collector Application prior to version v1.8.4 SOAR Plugin Application prior to version 5.3.1 Deployment Intelligence Application prior to 3.0.12 User Behavior Analytics Application add-on prior to 4.1.14 Pulse Application add-on prior to 2.2.12 Assistant Application add-on prior to 3.6.0 Use Case Manager Application add-on prior to 3.9.0 WinCollect Standalone Agent prior to 10.1.8 M7 Appliances prior to 4.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-50447)
Description	Oracle has issued security updates addressing an Arbitrary Code Execution Vulnerability that exists in Oracle Linux components. Pillow through 10.1.0 allows PIL.ImageMath.eval Arbitrary Code Execution via the environment parameter. Oracle advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Oracle Linux v8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/linuxbulletinjan2024.html

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2024-22436, CVE-2024-26303)
Description	HPE has released security updates addressing multiple Denial of Service Vulnerabilities that exist in HPE ArubaOS-Switches and IceWall products. **CVE-2024-22436** - A vulnerability exists in the SSH daemon in AOS-S switches. The vulnerability requires a specially crafted request sent to the device to be exploitable. Successful exploitation results in a Denial-of-Service condition. **CVE-2024-26303** - Authenticated Denial of Service Vulnerability in ArubaOS-Switch SSH Daemon. HPE advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Aruba 5400R Series Switches Aruba 3810 Series Switches Aruba 2920 Series Switches Aruba 2930F Series Switches Aruba 2930M Series Switches Aruba 2530 Series Switches Aruba 2540 Series Switches Aruba 3800 Series Switches ArubaOS-Switch 16.11.xxxx: KB/WC/YA/YB/YC.16.11.0015 and below. ArubaOS-Switch 16.10.xxxx: KB/WC/YA/YB/YC - All versions. ArubaOS-Switch 16.10.xxxx: WB.16.10.24 and below. ArubaOS-Switch 16.09.xxxx: All versions. ArubaOS-Switch 16.08.xxxx: All versions. ArubaOS-Switch 16.07.xxxx: All versions. ArubaOS-Switch 16.06.xxxx: All versions. ArubaOS-Switch 16.05.xxxx: All versions. ArubaOS-Switch 16.04.xxxx: KA/RA.16.04.0027 and below. ArubaOS-Switch 16.03.xxxx: All versions. ArubaOS-Switch 16.02.xxxx: All versions. ArubaOS-Switch 16.01.xxxx: All versions. ArubaOS-Switch 15.xx.xxxx: All versions. IceWall Gen11 Enterprise Edition 11.0 (Windows) - IceWall Gen11 Agent only IceWall Gen11 Standard Edition 11.0 (Windows) - IceWall Gen11 Agent only IceWall SSO Agent Option 10.0 (Windows)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04627en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbmu04626en_us

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39191, CVE-2023-46813, CVE-2023-51779, CVE-2023-6531)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in Linux Kernel RT. These vulnerabilities could be exploited by malicious users to allow Local Privilege Escalation, Arbitrary Code Execution, IO lock-ups and Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240995-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240991-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240986-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240989-1/ https://www.suse.com/support/update/announcement/2024/suse-ru-20240988-1/

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	Local Code Injection Vulnerability (CVE-2024-1417)
Description	WatchGuard has released a security update addressing a Local Code Injection Vulnerability that exists in AuthPoint Password Manager Extension for MacOS Safari. This could allow a local authenticated user to execute arbitrary commands. WatchGuard advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	AuthPoint Password Manager Extension for MacOS Safari Versions before 1.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00006

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27270, CVE-2024-28784, CVE-2023-50961, CVE-2023-50960, CVE-2022-26377)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Scripting and AJP Smuggling. IBM recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty version 23.0.0.3 - 24.0.0.3 IBM QRadar SIEM versions 7.5 - 7.5.0 UP7 IF06
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7145231 https://www.ibm.com/support/pages/node/7145260 https://www.ibm.com/support/pages/node/7145262 https://www.ibm.com/support/pages/node/7145265

Affected Product	**Oracle**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40225, CVE-2024-21319, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1551, CVE-2024-1552)
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in Oracle Linux components. These vulnerabilities could be exploited by malicious users to cause Identity Denial of service, User Interface Spoofing, session or cookie hijacking. Oracle recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Oracle Linux versions 7, 8, 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/linuxbulletinjan2024.html

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22463, CVE-2024-25964, CVE-2024-24901, CVE-2024-0162, CVE-2024-0163, CVE-2023-22655, CVE-2023-32666, CVE-2023-38575, CVE-2023-39368, CVE-2023-35191, CVE-2023-32282, CVE-2024-0154, CVE-2024-0173, CVE-2023-2222, CVE-2022-48064, CVE-2021-32256, CVE-2022-35205, CVE-2022-47673, CVE-2022-4285, CVE-2023-25585, CVE-2023-1579, CVE-2022-44840, CVE-2022-35206, CVE-2023-25588, CVE-2023-0687, CVE-2022-48065, CVE-2022-47695, CVE-2022-48063, CVE-2023-3341, CVE-2023-28840, CVE-2023-28841, CVE-2023-28842, CVE-2023-4813, CVE-2023-22081, CVE-2022-41974, CVE-2022-41973, CVE-2023-4389, CVE-2023-42753, CVE-2023-1206, CVE-2023-4921, CVE-2023-23454, CVE-2023-4623, CVE-2020-36766, CVE-2023-1859, CVE-2023-2177, CVE-2023-4881, CVE-2023-40283, CVE-2023-1192, CVE-2023-36054, CVE-2023-4039, CVE-2023-44487, CVE-2023-1829, CVE-2023-38408, CVE-2023-0215, CVE-2023-5678, CVE-2023-3817, CVE-2023-3446, CVE-2023-2650, CVE-2023-20900, CVE-2023-40217, CVE-2023-45803, CVE-2023-5535, CVE-2023-46246, CVE-2023-5441, CVE-2023-5344, CVE-2023-34326, CVE-2023-34327, CVE-2023-34328, CVE-2023-34323, CVE-2023-34325)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Sensitive Information Disclosure, Privilege Escalation, Denial of Service, out-of-bound read/write conditions. Dell recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerScale OneFS Versions 8.2.0 through 9.7.0.1 Multiple PowerEdge products Multiple XC Core products Multiple EMC XC Core products Multiple XC Hyper-converged Appliances Multiple PowerStore products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222691/dsa-2024-062-security-update-for-dell-powerscale-onefs-for-proprietary-code-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000222756/dsa-2024-003-security-update-for-dell-poweredge-server-bios-for-a-time-of-check-time-of-use-toctou-vulnerability https://www.dell.com/support/kbdoc/en-us/000222812/dsa-2024-004-security-update-for-dell-poweredge-server-bios-for-an-improper-smm-communication-buffer-verification-vulnerability https://www.dell.com/support/kbdoc/en-us/000222891/dsa-2024-005-security-update-for-dell-poweredge-server-for-intel-march-2024-security-advisories-2024-1-ipu https://www.dell.com/support/kbdoc/en-us/000222898/dsa-2024-034-security-update-for-dell-poweredge-server-bios-for-an-improper-parameter-initialization-vulnerability https://www.dell.com/support/kbdoc/en-us/000223033/dsa-2024-120-security-update-dell-powerstore-vulnerabilities

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0565, CVE-2024-26602)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Enterprise Linux kernel. **CVE-2024-0565** - An out-of-bounds memory read flaw was found in receive_encrypted_standard in fs/smb/client/smb2ops.c in the SMB Client sub-component in the Linux Kernel. This issue occurs due to integer underflow on the memcpy length, leading to a denial of service. **CVE-2024-26602** - A flaw was found in sys_membarrier in the Linux kernel in sched/membarrier in how a user calls it at too high of a frequency. This flaw allows a local user to saturate the machine. Red Hat recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1532 https://access.redhat.com/errata/RHSA-2024:1533

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.