Advisory Alert

Alert Number: AAA20240417 **Date:** April 17, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	Multiple Vulnerabilities
Palo Alto	**Critical**	Command Injection Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Ivanti	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Red Hat	Medium	Multiple Vulnerabilities

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released April 2024 Security Updates addressing multiple vulnerabilities in Oracle code and in third-party components included in Oracle products. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpuapr2024.html

Affected Product	**Palo Alto**
Severity	**Critical** - Initial release date **12th April 2024 (AAA20240415)**
Affected Vulnerability	Command Injection Vulnerability (CVE-2024-3400)
Description	Palo Alto has released security updates addressing a Command Injection Vulnerability that exists in the GlobalProtect feature of Palo Alto Networks PAN-OS software. If exploited it may allow an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS versions prior to 11.1.0-h3, 11.1.1-h1, 11.1.2-h3 PAN-OS versions prior to 11.0.2-h4, 11.0.3-h10, 11.0.4-h1 PAN-OS versions prior to 10.2.5-h6, 10.2.6-h3, 10.2.7-h8, 10.2.8-h3, 10.2.9-h1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-3400

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. Malicious users could exploit these vulnerabilities to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell custom VMware ESXi- ESXi 7.0U3-A19 and prior Dell custom VMware ESXi- ESXi 8.0U2-A05 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000224179/dsa-2024-182-security-update-for-dell-custom-vmware-esxi-vulnerabilities

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24996, CVE-2024-29204)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-24996** - A Heap overflow vulnerability in WLInfoRailService component of Ivanti Avalanche before 6.4.3 allows an unauthenticated remote attacker to execute arbitrary commands. **CVE-2024-29204** - A Heap Overflow vulnerability in WLAvalancheService component of Ivanti Avalanche before 6.4.3 allows a remote unauthenticated attacker to execute arbitrary commands. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Avalanche versions prior to 6.4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-5733,CVE-2019-6470,CVE-2021-25217,CVE-2022-2928,CVE-2022-2929,CVE-2024-0553,CVE-2023-5981,CVE-2023-36054,CVE-2023-22084,CVE-2021-39537,CVE-2023-29491,CVE-2020-11080,CVE-2023-44487,CVE-2022-48565,CVE-2022-48560,CVE-2022-48564,CVE-2022-48566,CVE-2023-40217,CVE-2023-3446,CVE-2023-3817,CVE-2019-19333,CVE-2019-19334,CVE-2019-20393,CVE-2019-20394,CVE-2019-20397,CVE-2019-20391,CVE-2019-20392,CVE-2019-20395,CVE-2019-20396,CVE-2019-20398,CVE-2019-11324,CVE-2023-43804,CVE-2018-25091,CVE-2019-11236,CVE-2020-26137,CVE-2023-45803,CVE-2023-7090,CVE-2023-28486,CVE-2023-28487)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products that in turn affect Dell products. Malicious users could exploit these vulnerabilities to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Networking OS10 version 10.5.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000224185/dsa-2024-180-security-update-for-dell-os10-third-party-vulnerabilities

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-46925,CVE-2021-46926,CVE-2021-46927,CVE-2021-46929,CVE-2021-46930,CVE-2021-46931,CVE-2021-46933,CVE-2021-46936,CVE-2021-47082,CVE-2021-47087,CVE-2021-47091,CVE-2021-47093,CVE-2021-47094,CVE-2021-47095,CVE-2021-47096,CVE-2021-47097,CVE-2021-47098,CVE-2021-47099,CVE-2021-47100,CVE-2021-47101,CVE-2021-47102,CVE-2021-47104,CVE-2021-47105,CVE-2021-47107,CVE-2021-47108,CVE-2022-48626,CVE-2022-48629,CVE-2022-48630,CVE-2023-35827,CVE-2023-52450,CVE-2023-52454,CVE-2023-52469,CVE-2023-52470,CVE-2023-52474,CVE-2023-52477,CVE-2023-52492,CVE-2023-52497,CVE-2023-52501,CVE-2023-52502,CVE-2023-52504,CVE-2023-52507,CVE-2023-52508,CVE-2023-52509,CVE-2023-52510,CVE-2023-52511,CVE-2023-52513,CVE-2023-52515,CVE-2023-52517,CVE-2023-52519,CVE-2023-52520,CVE-2023-52523,CVE-2023-52524,CVE-2023-52525,CVE-2023-52528,CVE-2023-52529,CVE-2023-52532,CVE-2023-52564,CVE-2023-52566,CVE-2023-52567,CVE-2023-52569,CVE-2023-52574,CVE-2023-52575,CVE-2023-52576,CVE-2023-52582,CVE-2023-52583,CVE-2023-52597,CVE-2023-52605,CVE-2023-52621,CVE-2024-25742,CVE-2024-26600,CVE-2023-52340,CVE-2024-0565,CVE-2024-1085,CVE-2023-42753)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Out-of-bounds memory read, Use-after-free condition, Memory leakage. Suse advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap Micro 5.3, 5.4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241320-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241318-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241312-1/

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22061, CVE-2024-23526, CVE-2024-23527, CVE-2024-23528, CVE-2024-23529, CVE-2024-23530, CVE-2024-23531, CVE-2024-23533, CVE-2024-23532, CVE-2024-23534, CVE-2024-23535, CVE-2024-24991, CVE-2024-24992, CVE-2024-24993, CVE-2024-24994, CVE-2024-24995, CVE-2024-24997, CVE-2024-24998, CVE-2024-24999, CVE-2024-25000, CVE-2024-27975, CVE-2024-27976, CVE-2024-27977, CVE-2024-27978, CVE-2024-27984)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Path Traversal, Use-After-Free Remote Code Execution, Null Pointer Dereference, Heap Overflow. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Avalanche versions prior to 6.4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22354, CVE-2024-22329)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-22354** - IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information, consume memory resources, or to conduct a server-side request forgery attack. **CVE-2024-22329** - IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker could exploit this vulnerability to conduct the SSRF attack. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 - 24.0.0.3 IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7148426 • https://www.ibm.com/support/pages/node/7148380

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33631, CVE-2023-6931)
Description	Red Hat has released security updates addressing a multiple vulnerabilities that exist in their products. **CVE-2021-33631** - A flaw was found in the openEuler kernel in Linux filesystem modules that allows an integer overflow via mounting a corrupted filesystem. **CVE-2023-6931** - A flaw was found in the Linux kernel's Performance Events system component. A condition can be triggered that allows data to be written past the end or before the beginning of the intended memory buffer. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:1840 • https://access.redhat.com/errata/RHSA-2024:1836

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.