Advisory Alert

Alert Number: **AAA20240418** **Date:** **April 18, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	SQL Injection Vulnerability
SUSE	**High**	Multiple Vulnerabilities
SolarWinds	**High**	Directory Traversal Remote Code Vulnerability
Cisco	**High, Medium**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Red Hat	**High, Medium**	Multiple Vulnerabilities
Oracle	**High, Medium, Low**	Multiple Vulnerabilities
f5	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	SQL Injection Vulnerability (CVE-2024-1597)
Description	Oracle has issued security updates addressing an SQL Injection Vulnerability that exists in Oracle Linux components. The PostgreSQL JDBC Driver, allows attacker to inject SQL if using PreferQueryMode=SIMPLE. By constructing a matching string payload, the attacker can inject SQL to alter the query, bypassing the protections that parameterized queries bring against SQL Injection attacks. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Linux 8,9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/linuxbulletinapr2024.html

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux kernel. If Exploited, these vulnerabilities could lead to Denial of Service, Privilege Escalation, memory leaks, use-after free issues, memory corruptions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5 openSUSE Leap Micro 5.3, 5.4 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5 SUSE Real Time Module 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/2024/suse-su-20241322-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241321-1/

Affected Product	**SolarWinds**
Severity	**High**
Affected Vulnerability	Directory Traversal Remote Code Vulnerability (CVE-2024-28073)
Description	SolarWinds has released security updates addressing a Directory Traversal Remote Code Vulnerability that exists in SolarWinds Serv-U servers. **CVE-2024-28073** - SolarWinds Serv-U was found to be susceptible to a Directory Traversal Remote Code Vulnerability. This vulnerability requires a highly privileged account to be exploited. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Serv-U 15.4.1.128 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28073

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20295, CVE-2024-20356, CVE-2024-20373)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If Exploited, these vulnerabilities could lead to Command Injection, Privilege Escalation and SNMP Polling. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco IOS and IOS XE 5000 Series Enterprise Network Compute Systems (ENCS) Catalyst 8300 Series Edge uCPE UCS C-Series Rack Servers in standalone mode UCS E-Series Servers UCS S-Series Storage Servers in standalone mode
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-mUx4c5AJ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-bLuPcb • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-uwBXfqww

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3341, CVE-2023-46218, CVE-2023-28322, CVE-2024-0553, 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-2023-22084, CVE-2023-7090, CVE-2023-28486, CVE-2023-28487, CVE-2023-48674)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell 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.dell.com/support/kbdoc/en-us/000224244/dsa-2024-183-security-update-for-dell-os10-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000220410/dsa-2023-467-security-update-for-a-dell-platform-bios-vulnerability

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22354, CVE-2024-22329, CVE-2023-50312, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20919, CVE-2024-20926, CVE-2024-20945, CVE-2023-33850)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere and PowerVM. These vulnerabilities could be exploited by malicious users to cause XML External Entity Injection, server-side request forgery Information Disclosure and high confidentiality and integrity impacts. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition v5.1 IBM WebSphere Application Server Liberty v17.0.0.3 - v24.0.0.3 IBM WebSphere Application Server 8.5, 9.0 PowerVM Novalink v2.0.0.0 - v2.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7148517 • https://www.ibm.com/support/pages/node/7148515 • https://www.ibm.com/support/pages/node/7148483 • https://www.ibm.com/support/pages/node/7148484

Affected Product	**Red Hat**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6240, CVE-2024-26582, CVE-2024-26584, CVE-2024-26586, CVE-2021-26341, CVE-2021-47099, CVE-2022-1184, CVE-2022-1852, CVE-2022-3640, CVE-2022-42895)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in Red Hat Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service, use-after-free conditions, Memory corruptions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 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 Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 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 CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 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 Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:1882 • https://access.redhat.com/errata/RHSA-2024:1881 • https://access.redhat.com/errata/RHSA-2024:1877

Affected Product	**Oracle**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released April 2024 Security Updates addressing multiple vulnerabilities that exist in Oracle Linux, VM server 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/linuxbulletinapr2024.html • https://www.oracle.com/security-alerts/bulletinapr2024.html • https://www.oracle.com/security-alerts/ovmbulletinapr2024.html

Affected Product	**f5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487, CVE-2022-38087)
Description	f5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-44487** - The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly. **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. f5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next (all modules) v20.0.1 - v20.0.2 and v15.1.0 - v15.1.10 NGINX Plus vR25 - vR30 NGINX Ingress Controller v3.0.0 - v3.3.0 F5OS-C v1.5.0 - v1.5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000137106 • https://my.f5.com/manage/s/article/K000134744

Affected Product	**Ubuntu**
Severity	**Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22705, CVE-2023-50431, CVE-2023-52429, CVE-2023-46838, CVE-2023-52436, CVE-2023-6610, CVE-2023-52438, CVE-2023-52434, CVE-2024-23850, CVE-2023-52439, CVE-2024-23851, CVE-2023-52435)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Sensitive Information Disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 23.10 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6724-2

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.