TLP: WHITE

Advisory Alert

Alert Number: **AAA20240314** **Date:** **March 14, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	LDAP Injection vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Red Hat	**High, Medium**	Multiple Vulnerabilities
Dell	**High, Medium, Low**	Multiple Vulnerabilities
Palo Alto	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36763, CVE-2022-36764, CVE-2022-40982, CVE-2022-43505, CVE-2023-32460, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237)
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in Dell PowerScale components. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Isilon A200 Versions prior to 12.1 Isilon A2000 Versions prior to 12.1 PowerScale Archive A300 Versions prior to 12.1 PowerScale Archive A3000 Versions prior to 12.1 Isilon H400 Versions prior to 12.1 Isilon H500 Versions prior to 12.1 Isilon H600 Versions prior to 12.1 Isilon H5600 Versions prior to 12.1 PowerScale Hybrid H700 Versions prior to 12.1 PowerScale Hybrid H7000 Versions prior to 12.1 PowerScale B100 Versions prior to 12.1 PowerScale F200 Versions prior to 12.1 PowerScale F600 Versions prior to 12.1 Isilon F800 Versions prior to 12.1 PowerScale F900 Versions prior to 12.1 PowerScale P100 Versions prior to 12.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222692/dsa-2024-090-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	LDAP Injection vulnerability (CVE-2022-46337)
Description	IBM has issued security updates addressing a LDAP Injection vulnerability that exists in IBM QRadar SIEM. **CVE-2022-46337** - Apache Derby could allow a remote attacker to bypass security restrictions, caused by a LDAP injection vulnerability in authenticator. By sending a specially crafted request, an attacker could exploit this vulnerability to view and corrupt sensitive data and run sensitive database functions and procedures. IBM advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar SIEM v7.5 - v7.5.0 UP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7140420

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-25162, CVE-2021-46923, CVE-2021-46924, CVE-2021-46932, CVE-2023-28746, CVE-2023-5197, CVE-2023-52340, CVE-2023-52429, CVE-2023-52439, CVE-2023-52443, CVE-2023-52445, CVE-2023-52447, CVE-2023-52448, CVE-2023-52449, CVE-2023-52451, CVE-2023-52452, CVE-2023-52456, CVE-2023-52457, CVE-2023-52463, CVE-2023-52464, CVE-2023-52475, CVE-2023-52478, CVE-2023-6817, CVE-2024-0607, CVE-2024-1151, CVE-2024-23849, CVE-2024-23850, CVE-2024-23851, CVE-2024-25744, CVE-2024-26585, CVE-2024-26586, CVE-2024-26589, CVE-2024-26591, CVE-2024-26593, CVE-2024-26595, CVE-2024-26598, CVE-2024-26602, CVE-2024-26603, CVE-2024-26622)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, use-after-free, information leak, kernel crash. SUSE advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP5 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 SUSE Linux Enterprise Workstation Extension 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240858-1/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20318, CVE-2024-20320, CVE-2024-20327, CVE-2024-20319, CVE-2024-20262, CVE-2024-20266, CVE-2024-20315, CVE-2024-20322, CVE-2023-20236)
Description	Cisco has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Denial of Service, Privilege Escalation, remote configuration bypass and installation of unverified software on affected devices. Cisco recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Cisco devices running on IOS XR 7.11 and earlier Multiple Cisco devices running on IOS XR 24.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrl2vpn-jesrU3fc https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ssh-privesc-eWDMKew3 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pppma-JKWFgneW https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-uhv6ZDeF https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-scp-dos-kb6sUUHw https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-dhcp-dos-3tgPKRdm https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-acl-bypass-RZU5NL3e https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ipxe-sigbypass-pymfyqgB

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952, CVE-2022-34169, CVE-2023-33850)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Denial of Service, arbitrary code execution, sensitive information disclosure and memory corruption. IBM recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM TXSeries for Multiplatforms v8.1, v8.2, v9.1 IBM QRadar SIEM v7.5 - v7.5.0 UP7 Rational Application Developer v9.6, v9.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7109966 https://www.ibm.com/support/pages/node/7140420 https://www.ibm.com/support/pages/node/7140984

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0480, CVE-2022-3545, CVE-2022-38096, CVE-2022-40982, CVE-2022-42896, CVE-2023-1192, CVE-2023-2163, CVE-2023-2166, CVE-2023-2176, CVE-2023-31436, CVE-2023-3268, CVE-2023-3390, CVE-2023-3609, CVE-2023-4459, CVE-2023-45871, CVE-2023-4622, CVE-2023-4921, CVE-2023-5717, CVE-2023-6546, CVE-2023-6932, CVE-2023-7192, CVE-2023-38409, CVE-2023-40283, CVE-2024-0646)
Description	Red Hat has released security updates addressing multiple vulnerabilities in Red Hat Linux kernel. If exploited, these vulnerabilities could lead to Privilege Escalation, memory exhaustion, use-after-free flaws, memory leak. Red Hat recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 and 9.2 x86_64, Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 and 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1323 https://access.redhat.com/errata/RHSA-2024:1306 https://access.redhat.com/errata/RHSA-2024:1303

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2022-43505, CVE-2022-40982, CVE-2022-36763, CVE-2022-36764, CVE-2023-32460, CVE-2024-0161, CVE-2024-0158, CVE-2024-0162, CVE-2024-0154, CVE-2024-0173)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could allow a local low privileged attacker to compromise the affected systems. Dell recommends to apply security fixes at your earliest to protect your systems from potential threats.
.Affected Products	Precision 7920 Rack versions prior to 2.21.2 7920 XL Rack versions prior to 2.21.2 Precision 7960 Rack versions prior to 2.0.0 Precision 7960 XL Rack versions prior to 2.0.0 Alienware m16 R1 BIOS Versions prior to 1.15.0 Alienware m18 R1 BIOS Versions prior to 1.15.0 ChengMing 3900 BIOS Versions prior to 1.20.0 Edge Gateway 3000 series BIOS Versions prior to 1.17.0 Inspiron 13 5310 BIOS Versions prior to 2.26.0 Inspiron 13 5320 BIOS Versions prior to 1.17.0 Inspiron 13 5330 BIOS Versions prior to 1.13.1 Inspiron 14 5410/5418 BIOS Versions prior to 2.25.0 Inspiron 14 5420 BIOS Versions prior to 1.20.0 Inspiron 14 5430 BIOS Versions prior to 1.12.0 Inspiron 14 7420 2-in-1 BIOS Versions prior to 1.18.0 Inspiron 14 7430 2-in-1 BIOS Versions prior to 1.12.0 Inspiron 14 Plus 7420 BIOS Versions prior to 1.21.0 Inspiron 14 Plus 7430 BIOS Versions prior to 1.13.0 Inspiron 15 5510/5518 BIOS Versions prior to 2.25.0 Inspiron 15 7510 BIOS Versions prior to 1.22.0 Inspiron 16 5620 BIOS Versions prior to 1.20.0 Inspiron 16 5630 BIOS Versions prior to 1.12.0 Inspiron 16 7610 BIOS Versions prior to 1.22.0 Inspiron 16 7620 2-in-1 BIOS Versions prior to 1.18.0 Inspiron 16 7630 2-in-1 BIOS Versions prior to 1.12.0 Inspiron 16 Plus 7620 BIOS Versions prior to 1.21.0 Inspiron 16 Plus 7630 BIOS Versions prior to 1.13.0 Inspiron 24 5420 All-in-One BIOS Versions prior to 1.9.0 Inspiron 27 7720 All-in-One BIOS Versions prior to 1.9.0 Inspiron 3891 BIOS Versions prior to 1.23.0 Inspiron 5400/5401 BIOS Versions prior to 1.26.0 Inspiron 5401 AIO BIOS Versions prior to 1.26.0 Inspiron 5410 BIOS Versions prior to 2.25.0 Inspiron 7700 All-In-One BIOS Versions prior to 1.26.0 Latitude 3320 BIOS Versions prior to 1.28.0 Latitude 3330 BIOS Versions prior to 1.20.0 Latitude 3340 BIOS Versions prior to 1.11.0 Latitude 3420 BIOS Versions prior to 1.35.0 Latitude 3440 BIOS Versions prior to 1.11.0 Latitude 3520 BIOS Versions prior to 1.35.0 Latitude 3540 BIOS Versions prior to 1.11.0 Latitude 5420 Rugged BIOS Versions prior to 1.31.0 Latitude 5424 Rugged BIOS Versions prior to 1.31.0 Latitude 7210 2-in-1 BIOS Versions prior to 1.28.0 Latitude 7424 Rugged Extreme BIOS Versions prior to 1.31.0 Latitude 9430 BIOS Versions prior to 1.21.1 Latitude 9510 2in1 BIOS Versions prior to 1.26.0 OptiPlex 3000 Micro / OptiPlex 3000 Small Form Factor / OptiPlex 3000 Tower BIOS Versions prior to 1.20.0 OptiPlex 5000 Micro / OptiPlex 5000 Small Form Factor / OptiPlex 5000 Tower BIOS Versions prior to 1.20.0 OptiPlex 5090 Micro / OptiPlex 5090 Small Form Factor / OptiPlex 5090 Tower BIOS Versions prior to 1.23.0 Precision 3260 XE Compact / Precision 3260 Compact BIOS Versions prior to 3.2.0 Precision 3460 XE Small Form Factor / Precision 3460 Small Form Factor BIOS Versions prior to 3.2.0 Precision 3640 BIOS Versions prior to 1.29.0 Precision 5550 BIOS Versions prior to 1.27.0 Precision 5770 BIOS Versions prior to 1.23.0 Precision 7865 Tower BIOS Versions prior to 1.7.0 Vostro 13 5310 BIOS Versions prior to 2.26.0 Vostro 14 5410 BIOS Versions prior to 2.25.0 Vostro 15 5510 BIOS Versions prior to 2.25.0 Vostro 15 7510 BIOS Versions prior to 1.22.0 Vostro 16 5630 BIOS Versions prior to 1.12.0 Vostro 3690 BIOS Versions prior to 1.23.0 Vostro 3890 BIOS Versions prior to 1.23.0 Vostro 5320 BIOS Versions prior to 1.17.0 Vostro 5890 BIOS Versions prior to 1.23.0 Vostro 7620 BIOS Versions prior to 1.21.0 Wyse 5070 BIOS Versions prior to 1.29.0 Wyse 5470 BIOS Versions prior to 1.24.0 Wyse 5470 All-In-One BIOS Versions prior to 1.25.0 XPS 13 9305 BIOS Versions prior to 1.20.0 XPS 13 7390 BIOS Versions prior to 1.24.0 XPS 13 7390 2-in-1 BIOS Versions prior to 1.30.0 XPS 15 7590 BIOS Versions prior to 1.27.0 XPS 15 9500 BIOS Versions prior to 1.27.0 XPS 17 9720 BIOS Versions prior to 1.23.0 XPS 17 9730 BIOS Versions prior to 1.10.0 XPS 9315 2-in-1 BIOS Versions prior to 1.14.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222319/dsa-2024-037 https://www.dell.com/support/kbdoc/en-us/000220141/dsa-2023-462 https://www.dell.com/support/kbdoc/en-us/000219967/dsa-2023-447 https://www.dell.com/support/kbdoc/en-us/000219973/dsa-2023-452 https://www.dell.com/support/kbdoc/en-us/000219971/dsa-2023-451

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-2433, CVE-2024-2432, CVE-2024-2431)
Description	Palo Alto has released security updates addressing multiple vulnerabilities that exist in PAN-OS and GlobalProtect App. If exploited, these vulnerabilities could lead to Local Privilege Escalation, Availability Loss and unauthorized access or control over the applications. **CVE-2024-2433** - An improper authorization vulnerability in Palo Alto Networks Panorama software enables an authenticated read-only administrator to upload files using the web interface and completely fill one of the disk partitions with those uploaded files, which prevents the ability to log into the web interface or to download PAN-OS, WildFire, and content images. **CVE-2024-2432** - A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privileges. However, execution requires that the local user is able to successfully exploit a race condition. **CVE-2024-2431** - An issue in the Palo Alto Networks GlobalProtect app enables a non-privileged user to disable the GlobalProtect app without needing the passcode in configurations that allow a user to disable GlobalProtect with a passcode. Palo Alto recommends to apply security fixes at your earliest to protect your systems from potential threats.
.Affected Products	PAN-OS 11.0 versions prior to 11.0.3 on Panorama PAN-OS 10.2 versions prior to 10.2.8 on Panorama PAN-OS 10.1 versions prior to 10.1.12 on Panorama PAN-OS 9.1 versions prior to 9.1.17 on Panorama PAN-OS 9.0 versions prior to 9.0.17-h4 on Panorama GlobalProtect App 5.1 versions prior to 5.1.12 GlobalProtect App 5.2 versions prior to 5.2.13 GlobalProtect App 6.0 versions prior to 6.0.8 on Windows GlobalProtect App 6.0 versions prior to 6.0.4 GlobalProtect App 6.1 versions prior to 6.1.2 on Windows GlobalProtect App 6.1 versions prior to 6.1.1 GlobalProtect App 6.2 versions prior to 6.2.1 on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2024-2433 https://security.paloaltonetworks.com/CVE-2024-2432 https://security.paloaltonetworks.com/CVE-2024-2431

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4134, CVE-2023-22995, CVE-2023-51782, CVE-2024-0607, CVE-2023-46862, CVE-2023-6121, CVE-2024-0340, CVE-2023-46343, CVE-2023-51779)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. If exploited, these vulnerabilities could lead to Denial of Service, arbitrary code execution and sensitive information disclosure. Ubuntu recommends to apply security fixes at your earliest to protect your systems from potential threats.
.Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6686-2

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.