Advisory Alert

Alert Number: AAA20241018 **Date:** October 18, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Externally-Controlled Format String Vulnerability
IBM	**Critical**	Use-after-free Vulnerability
Oracle	**Critical**	Security Update
SolarWinds	**Critical**	Java Deserialization Remote Code Execution Vulnerability
VMware Broadcom	**High**	Authenticated SQL Injection Vulnerability
Dell	**High**	Multiple Vulnerabilities
Juniper	**High**	Blast-RADIUS Vulnerability
SUSE	**High**	Multiple Vulnerabilities
SolarWinds	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Denial of Service Vulnerability
Oracle	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Improper Error Handling Vulnerability
cPanel	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Secure Connect Gateway and Secure Connect Gateway Policy Manager. 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	Dell Secure Connect Gateway Version 5.24.00.14 Dell Policy Manager for Secure Connect Gateway Version 5.24.00.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000237211/dsa-2024-407-dell-secure-connect-gateway-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000236839/dsa-2024-406-security-update-for-dell-secure-connect-gateway-policy-manager-multiple-vulnerabilities

Affected Product	**FortiGuard**
Severity	**Critical -** Initial release date **9th Feb 2024 (AAA20240306)**
Affected Vulnerability	Externally-Controlled Format String Vulnerability (CVE-2024-23113)
Description	FortiGuard has released security updates addressing an Externally-Controlled Format String Vulnerability that exists in their products. **CVE-2024-23113** - A use of externally-controlled format string vulnerability in FortiOS fgfmd daemon may allow a remote unauthenticated attacker to execute arbitrary code or commands via specially crafted requests. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiOS 7.4 versions 7.4.0 through 7.4.2 FortiOS 7.2 versions 7.2.0 through 7.2.6 FortiOS 7.0 versions 7.0.0 through 7.0.13 FortiPAM 1.2 all versions FortiPAM 1.1 all versions FortiPAM 1.0 all versions FortiProxy 7.4 versions 7.4.0 through 7.4.2 FortiProxy 7.2 versions 7.2.0 through 7.2.8 FortiProxy 7.0 versions 7.0.0 through 7.0.15 FortiSwitchManager 7.2 versions 7.2.0 through 7.2.3 FortiSwitchManager 7.0 versions 7.0.0 through 7.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-24-029

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2018-1311)
Description	IBM has released security updates addressing a Use-after-free Vulnerability that exists in Apache Xerces-C which affects IBM QRadar modules. **CVE-2018-1311** - Apache Xerces-C could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free error during the scanning of external DTDs. By sending a specially crafted file, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP9 IF03 QRadar Incident Forensics versions 7.5 - 7.5.0 UP9 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7173420

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-3596)
Description	Oracle has released a security update addressing a vulnerability that exists in Oracle Linux. This vulnerability could be exploited by malicious users to compromise the affected system. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Linux 7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/linuxbulletinoct2024.html

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Java Deserialization Remote Code Execution Vulnerability (CVE-2024-28988)
Description	SolarWinds has released security updates addressing a Java Deserialization Remote Code Execution vulnerability that exists in SolarWinds Web Help Desk. **CVE-2024-28988** - SolarWinds Web Help Desk was found to be susceptible to a Java Deserialization Remote Code Execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. This vulnerability was found by the ZDI team after researching a previous vulnerability and providing this report. The ZDI team was able to discover an unauthenticated attack during their research. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Web Help Desk 12.8.3 HF2 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28988

Affected Product	**VMware Broadcom**
Severity	**High**
Affected Vulnerability	Authenticated SQL Injection Vulnerability (CVE-2024-38814)
Description	Broadcom has released security updates addressing an Authenticated SQL Injection Vulnerability that exist in VMware HCX. A malicious authenticated user with non-administrator privileges may be able to enter specially crafted SQL queries and perform unauthorized remote code execution on the HCX manager. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware HCX 4.10.x, 4.9.x and 4.8.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25019

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45766, CVE-2024-45767, CVE-2023-22351, CVE-2023-25546, CVE-2023-41833, CVE-2023-43753, CVE-2023-42772, CVE-2024-21781, CVE-2024-21829, CVE-2024-21871, CVE-2024-23599, CVE-2024-24968, CVE-2024-23984)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell OpenManage Enterprise and Dell Precision Rack. 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	Dell OpenManage Enterprise versions prior to 4.2.0 Precision 7920 Rack BIOS versions prior to 2.22.2 7920 XL Rack BIOS versions prior to 2.22.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000237300/dsa-2024-426-security-update-for-dell-openmanage-enterprise-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227017/dsa-2024-329

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Blast-RADIUS Vulnerability (CVE-2024-3596)
Description	Juniper has released security updates addressing an Authentication Bypass by Spoofing vulnerability that exist in RADIUS protocol of Juniper Networks platforms. This allows an on-path attacker between RADIUS server and a RADIUS client to bypass authentication when RADIUS authentication is in use. This vulnerability depends on using the MD5 hash function to pass undetected attribute forgery by modifying RADIUS server Responses (Access-Accept, Access-Reject, or Access-Challenge). The attacker does not learn user credentials. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following products which use RADIUS implementation or any other affected implementations; Juniper Networks Junos OS • All versions before 21.4R3-S9 • 22.2 before 22.2R3-S5 • 22.4 before 22.4R3-S5 • 23.2 before 23.2R2-S3 • 23.4 before 23.4R2-S3 • 24.2 before 24.2R2 Juniper Networks Junos OS Evolved • All versions before 21.4R3-S9-EVO • 22.2 before 22.2R3-S5-EVO • 22.3 before 22.3R3-S4-EVO • 22.4 before 22.4R3-S5-EVO • 23.2 before 23.2R2-S3-EVO • 23.4 before 23.4R2-S3-EVO • 24.2 before 24.2R2-EVO Juniper Networks cRPD • 23.4 version and later versions before 23.4R2-S3 • 24.2 before 24.2R2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-09-30-Out-of-Cycle-Security-Advisory-Multiple-Products-RADIUS-protocol-susceptible-to-forgery-attacks-Blast-RADIUS-CVE-2024-3596?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52846, CVE-2024-26828, CVE-2024-26923, CVE-2024-27398, CVE-2024-35861, CVE-2024-36899, CVE-2024-36964, CVE-2024-40954, CVE-2024-41059, CVE-2024-40909, CVE-2021-47291)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.3, 15.4, 15.5, 15.6 SUSE Linux Enterprise High Performance Computing 15 SP2, SP3, SP4, SP5 SUSE Linux Enterprise Live Patching 15-SP2, SP3, SP4, SP5, SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, SP5,SP6 SUSE Linux Enterprise Server 15 SP2, SP3, SP4, SP5, SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP2, SP3, SP4, SP5, SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243710-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243706-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243708-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243707-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243704-1/

Affected Product	**SolarWinds**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45715, CVE-2024-45710, CVE-2024-45713, CVE-2024-45714, CVE-2024-45711)
Description	SolarWinds 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, Local Privilege Escalation, Sensitive Information Disclosure, Directory Traversal, and Remote Code Execution. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Platform 2024.2.1 and previous versions Serv-U 15.4.2.3 and previous versions Kiwi CatTools 3.12 and previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45715 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45710 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45714 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45711 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-45713

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20420, CVE-2024-20421, CVE-2024-20458, CVE-2024-20459, CVE-2024-20460, CVE-2024-20461, CVE-2024-20462, CVE-2024-20463, CVE-2024-20512, CVE-2024-20280)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Request Forgery, Information Disclosure, Command Injection, Cross-Site Scripting, Denial of Service, and Privilege Escalation. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Unified CCMP 12.6 Cisco UCS Central version 2.0 and earlier ATA 191 Analog Telephone Adapter versions 12.0.1 and earlier ATA 191 and 192 Multiplatform Analog Telephone Adapter versions 11.2.4 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multi-RDTEqRsy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccmpdm-rxss-tAX76U3k • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsc-bkpsky-TgJ5f73J

Affected Product	**Oracle**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3446, CVE-2024-23185, CVE-2024-41090, CVE-2024-41091, CVE-2024-41090, CVE-2024-41091, CVE-2024-41090, CVE-2024-41091, CVE-2024-21823, CVE-2024-7529, CVE-2024-8386, CVE-2024-8386, CVE-2024-40942)
Description	Oracle 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. Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Linux 7, 8, 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/linuxbulletinoct2024.html

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27397, CVE-2024-45016, CVE-2024-26960, CVE-2024-38630)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7073-1 • https://ubuntu.com/security/notices/USN-7072-1 • https://ubuntu.com/security/notices/USN-7071-1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Denial of Service, Arbitrary Code Execution, Cross-site Scripting, session hijacking. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP9 IF03 QRadar Incident Forensics versions 7.5 - 7.5.0 UP9 IF03 IBM QRadar Network Packet Capture versions 7.5.0 - 7.5.0 Update Package 9 IBM Storage Defender - Data Protect versions 1.0.0 - 1.4.1 IBM Storage Scale System versions 6.1.0.0 - 6.1.9.3 and 6.2.0.0 - 6.2.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173420 • https://www.ibm.com/support/pages/node/7173421 • https://www.ibm.com/support/pages/node/7091980 • https://www.ibm.com/support/pages/node/7150684 • https://www.ibm.com/support/pages/node/7173184

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Improper Error Handling Vulnerability
Description	Drupal has released security updates addressing an Improper Error Handling Vulnerability that exist in certain Drupal core module. Under certain uncommon site configurations, a bug in the CKEditor 5 module can cause some image uploads to move the entire webroot to a different location on the file system. This could be exploited by a malicious user to take down a site. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal core versions 10.0 up to 10.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2024-002

Affected Product	**cPanel**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Data modification. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	cPanel 110 Release: versions prior to 11.110.0.44 cPanel 118 Release: versions prior to 11.118.0.20 cPanel 122 Release: versions prior to 11.122.0.20 cPanel 124 Release: versions prior to 11.124.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/target-security-release-2024-0001-disclosure/

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.