TLP: WHITE

Advisory Alert

Alert Number: AAA20241211 **Date:** December 11, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
SAP	**High**, Medium, Low	Multiple Vulnerabilities
IBM	Medium	Multiple Denial of Service Vulnerabilities
Red Hat	Medium, Low	Multiple Vulnerabilities
cPanel	Low	Security Update

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-11633, CVE-2024-11634)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-11633** - Argument injection in Ivanti Connect Secure before version 22.7R2.4 allows a remote authenticated attacker with admin privileges to achieve remote code execution **CVE-2024-11634** - Command injection in Ivanti Connect Secure before version 22.7R2.3 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated attacker with admin privileges to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure (ICS) versions 22.7R2.3 and prior Ivanti Policy Secure (IPS) versions 22.7R1.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Connect-Secure-ICS-and-Ivanti-Policy-Secure-IPS-Multiple-CVEs?language=en_US

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47578, CVE-2024-47579, CVE-2024-47580)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. **CVE-2024-47578** - Adobe Document Service allows an attacker with administrator privileges to send a crafted request from a vulnerable web application. It is usually used to target internal systems behind firewalls that are normally inaccessible to an attacker from the external network, resulting in a Server-Side Request Forgery vulnerability. On successful exploitation, the attacker can read or modify any file and/or make the entire system unavailable. **CVE-2024-47579** - An attacker authenticated as an administrator can use an exposed webservice to upload or download a custom PDF font file on the system server. Using the upload functionality to copy an internal file into a font file and subsequently using the download functionality to retrieve that file allows the attacker to read any file on the server with no effect on integrity or availability **CVE-2024-47580** - An attacker authenticated as an administrator can use an exposed webservice to create a PDF with an embedded attachment. By specifying the file to be an internal server file and subsequently downloading the generated PDF, the attacker can read any file on the server with no effect on integrity or availability. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP NetWeaver AS for JAVA (Adobe Document Services) Versions - ADSSSAP 7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2024.html

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-49105, CVE-2024-49138, CVE-2024-49116, CVE-2024-49112, CVE-2024-49110, CVE-2024-49088, CVE-2024-49081, CVE-2024-49077, CVE-2024-43600, CVE-2024-49142, CVE-2024-49125, CVE-2024-49124, CVE-2024-49121, CVE-2024-49108, CVE-2024-49107, CVE-2024-49102, CVE-2024-49097, CVE-2024-49091, CVE-2024-49089, CVE-2024-49084, CVE-2024-49128, CVE-2024-49127, CVE-2024-49118, CVE-2024-49114, CVE-2024-49113, CVE-2024-49109, CVE-2024-49095, CVE-2024-49090, CVE-2024-49083, CVE-2024-49082, CVE-2024-49080, CVE-2024-49079, CVE-2024-49078, CVE-2024-49076, CVE-2024-49075, CVE-2024-49072, CVE-2024-49065, CVE-2024-49063, CVE-2024-49062, CVE-2024-49132, CVE-2024-49129, CVE-2024-49126, CVE-2024-49123, CVE-2024-49122, CVE-2024-49120, CVE-2024-49119, CVE-2024-49117, CVE-2024-49115, CVE-2024-49111, CVE-2024-49106, CVE-2024-49104, CVE-2024-49103, CVE-2024-49101, CVE-2024-49099, CVE-2024-49098, CVE-2024-49096, CVE-2024-49094, CVE-2024-49093, CVE-2024-49092, CVE-2024-49087, CVE-2024-49086, CVE-2024-49085, CVE-2024-49074, CVE-2024-49073, CVE-2024-49070, CVE-2024-49069, CVE-2024-49068, CVE-2024-49064, CVE-2024-49059, CVE-2024-49057, CVE-2024-43594, CVE-2024-12053, CVE-2024-49041)
Description	Microsoft has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Denial of Service, Privilege Escalation, Information Disclosure. Microsoft advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Windows App Client for Windows Desktop Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 (Server Core installation) Windows Server 2012 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 for 32-bit Systems Windows Server 2025 Windows 11 Version 24H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows Server 2022, 23H2 Edition (Server Core installation) Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows Server 2025 (Server Core installation) Windows 10 Version 22H2 for 32-bit Systems Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows Server 2022 (Server Core installation) Windows Server 2022 Remote Desktop client for Windows Desktop Windows Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Microsoft Office 2016 (32-bit edition) Microsoft Project 2016 (64-bit edition) Microsoft Project 2016 (32-bit edition) Microsoft Access 2016 (64-bit edition) Microsoft Access 2016 (32-bit edition) Microsoft Office LTSC 2024 for 64-bit editions Microsoft Office LTSC 2024 for 32-bit editions Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for 32-bit Systems Service Pack 2 Microsoft Word 2016 (64-bit edition) Microsoft Word 2016 (32-bit edition) Microsoft Office LTSC for Mac 2024 Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft Office 2019 for 64-bit editions Microsoft Office 2019 for 32-bit editions Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016 Microsoft/Muzic Microsoft SharePoint Server Subscription Edition Microsoft Office 2016 (64-bit edition) Microsoft Excel 2016 (64-bit edition) Microsoft Excel 2016 (32-bit edition) Microsoft Defender for Endpoint for Android System Center Operations Manager (SCOM) 2025 System Center Operations Manager (SCOM) 2022 System Center Operations Manager (SCOM) 2019 Microsoft Edge (Chromium-based)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Dec

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47598, CVE-2023-52752, CVE-2023-52846, CVE-2024-26923, CVE-2024-35861, CVE-2024-35862, CVE-2024-35864, CVE-2024-35950, CVE-2024-36899, CVE-2024-36904, CVE-2024-36964, CVE-2024-40954, CVE-2024-41059, CVE-2024-43861)
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 15.4 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP4 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP2, 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244275-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244276-1/

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-8540, CVE-2024-7572, CVE-2024-10256, CVE-2024-37377, CVE-2024-9844, CVE-2024-37401)
Description	Ivanti 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, bypass restrictions and modification of sensitive application components. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Sentry versions 9.20.1 and prior, 10.0.1 and prior Ivanti Desktop and Server Management (DSM) v2024.2 Ivanti Endpoint Manager (EPM) 2024 September Security Update and prior, 2022 SU6 and prior Ivanti Security Controls (iSec) versions 2024.3.2 (9.6.9365.0) and prior Ivanti Patch for Configuration Manager versions 2024.3 (2.5.1058) and prior Ivanti Neurons for Patch Management versions 2024.3 (1.1.55.0) and prior Ivanti Neurons Agent Platform versions 2024.1 (9.6.771.) and prior Ivanti Connect Secure (ICS) versions 22.7R2.3 and prior Ivanti Policy Secure (IPS) versions 22.7R1.1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Sentry-CVE-2024-8540?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Desktop-and-Server-Management-DSM-CVE-2024-7572?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Patch-SDK-CVE-2024-10256?language=en_US • https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Connect-Secure-ICS-and-Ivanti-Policy-Secure-IPS-Multiple-CVEs?language=en_US

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-54008, CVE-2022-25844)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE Aruba Networking AirWave Management Platform. **CVE-2022-25844 -** The package angular after 1.7.0 are vulnerable to Regular Expression Denial of Service (ReDoS) by providing a custom locale rule that makes it possible to assign the parameter in posPre: ' '.repeat() of NUMBER_FORMATS.PATTERNS[1].posPre with a very high value. **CVE-2024-54008** - An authenticated Remote Code Execution (RCE) vulnerability exists in the AirWave CLI. Successful exploitation of this vulnerability could allow a remote authenticated threat actor to run arbitrary commands as a privileged user on the underlying host. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking AirWave Management Platform versions 8.3.0.3 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04765en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22185, CVE-2024-24985, CVE-2023-52340, CVE-2024-42154, CVE-2024-21944)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell 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	BIOS Versions prior to 2.4.4 running on Precision 7960 Rack and Precision 7960 XL Rack DRAC9 firmware version prior to 7.00.00.174 running on Precision 7920 Rack and 7920 XL Rack BIOS Versions prior to 1.5.5 running on PowerEdge C6615 BIOS Versions prior to 1.10.5 running on • PowerEdge R6615 • PowerEdge R7615 • PowerEdge R6625 • PowerEdge R7625 • Dell XC Core XC7625 BIOS Versions prior to 2.17.0 running on • PowerEdge R6515 • PowerEdge R7515 • PowerEdge C6525 BIOS Versions prior to 2.17.4 running on • PowerEdge R6525 • PowerEdge R7525 • Dell EMC XC Core XC7525
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000244468/dsa-2024-442 • https://www.dell.com/support/kbdoc/en-us/000242188/dsa-2024-434 • https://www.dell.com/support/kbdoc/en-us/000258735/dsa-2024-404-security-update-for-dell-amd-based-poweredge-server-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41095, CVE-2022-48943, CVE-2024-46757, CVE-2024-46759, CVE-2024-35877, CVE-2024-42104, CVE-2024-42310, CVE-2024-41059, CVE-2024-38538, CVE-2023-52599, CVE-2024-26675, CVE-2024-26633, CVE-2024-26668, CVE-2023-52531, CVE-2023-52502, CVE-2024-38560, CVE-2024-42309, CVE-2024-42240, CVE-2024-46758, CVE-2024-43882, CVE-2023-52614, CVE-2021-47055, CVE-2024-46756, CVE-2024-26636, CVE-2024-46723, CVE-2024-46738, CVE-2024-44998, CVE-2024-46743, CVE-2024-41071, CVE-2022-24448, CVE-2024-41089, CVE-2022-48733, CVE-2024-46800, CVE-2023-52578, CVE-2024-44942, CVE-2024-44987, CVE-2024-46722, CVE-2024-27397, CVE-2022-48938, CVE-2024-42244)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux Kernel. 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 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7148-1

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47590, CVE-2024-54198, CVE-2024-47586, CVE-2024-54197, CVE-2024-47582, CVE-2024-32732, CVE-2024-47585, CVE-2024-42375, CVE-2024-28166, CVE-2024-41731, CVE-2024-47581, CVE-2024-47576, CVE-2024-47577)
Description	SAP has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Cross-Site Scripting, Information Disclosure, Server-Side Request Forgery, DLL Hijacking. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP Web Dispatcher, Versions – WEBDISP 7.77, 7.89, 7.93, KERNEL 7.77, 7.89, 7.93, 9.12, 9.13 • SAP NetWeaver Application Server ABAP, Version – KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93 • AP NetWeaver Application Server for ABAP and ABAP Platform, Versions – KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, 8.04, KERNEL 7.22, 7.53, 7.54, 7.77, 7.89, 7.93, 8.04, 9.12, 9.13 • SAP NetWeaver Administrator (System Overview), Version – LM-CORE 7.50 SAP NetWeaver AS JAVA, Version – LM-CORE 7.50 • SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions – SAP_BASIS 740, SAP_BASIS 750 • SAP BusinessObjects Business Intelligence Platform, Versions – ENTERPRISE 430, 2025 • SAP HCM, Version – S4HCMGXX 101 • SAP Product Lifecycle Costing, Version - PLC_CLIENT 4 • SAP Commerce Cloud, Versions - HY_COM 2205, COM_CLOUD 2211
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/december-2024.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Denial of Service Vulnerabilities (CVE-2024-37071, CVE-2024-45663, CVE-2024-41762, CVE-2024-41761)
Description	IBM has released security updates addressing Multiple Denial of Service Vulnerabilities that exist in IBM Db2. These vulnerabilities could be exploited by malicious users to compromise the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 versions 10.5.0 - 10.5.11, 11.1.4 - 11.1.4.7, 11.5.0 - 11.5.9, 12.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7175940 • https://www.ibm.com/support/pages/node/7175943 • https://www.ibm.com/support/pages/node/7175946 • https://www.ibm.com/support/pages/node/7175947

Affected Product	**Red Hat**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38564, CVE-2024-46695, CVE-2024-49949, CVE-2024-50082, CVE-2024-50099, CVE-2024-50110, CVE-2024-50142, CVE-2024-50192, CVE-2024-50256, CVE-2024-50264, CVE-2023-51779, CVE-2024-26830, CVE-2024-26615, CVE-2024-43854, CVE-2024-44994, CVE-2024-45018, CVE-2024-50251, CVE-2024-4109)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64, RHEL 8 x86_64, RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64, 9.2 aarch64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64, 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le, 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64, 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64, 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64, 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 8 aarch64, 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x, 9.2 s390x Red Hat Enterprise Linux for IBM z Systems 8 s390x, 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le, 9 ppc64le Red Hat Enterprise Linux for Real Time 8 x86_64, 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64, 9 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 Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64, 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64, 9.2 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64, 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:10946 • https://access.redhat.com/errata/RHSA-2024:10945 • https://access.redhat.com/errata/RHSA-2024:10944 • https://access.redhat.com/errata/RHSA-2024:10943 • https://access.redhat.com/errata/RHSA-2024:10941 • https://access.redhat.com/errata/RHSA-2024:10939 • https://access.redhat.com/errata/RHSA-2024:10933 • https://access.redhat.com/errata/RHSA-2024:10929 • https://access.redhat.com/errata/RHSA-2024:10928 • https://access.redhat.com/errata/RHSA-2024:10927

Affected Product	**cPanel**
Severity	**Low**
Affected Vulnerability	Security Update
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in cPanel & WHM product. These vulnerabilities could be exploited by malicious users to compromise the affected system. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	The following cPanel & WHM versions prior to, 124.0.21 118.0.30 110.0.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/targeted-security-release-2024-0002-announcement/

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.