Advisory Alert

Alert Number: AAA20240814 **Date:** August 14, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Use-after-free Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
SAP	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
F5	**Medium**	Server-Side Request Forgery
Fortiguard	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-7593, CVE-2024-7569)
Description	Ivanti has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2024-7593 -** Incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2 allows a remote unauthenticated attacker to bypass authentication of the admin panel. **CVE-2024-7569 -** An information disclosure vulnerability in Ivanti ITSM on-prem and Neurons for ITSM versions 2023.4 and earlier allows an unauthenticated attacker to obtain the OIDC client secret via debug information. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Virtual Traffic Manager - 22.2 Ivanti Virtual Traffic Manager - 22.7R1 Ivanti Neurons for ITSM - 2023.2, 2023.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2024-7569-CVE-2024-7570?language=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2023-4623)
Description	IBM has released security updates addressing a Use-after-free Vulnerability that exists in IBM Storage Defender. **CVE-2023-4623** - Linux Kernel could allow a local authenticated attacker to gain elevated privileges on the system, caused by a use-after-free flaw in the net/sched: sch_hfsc (HFSC qdisc traffic control) component. By sending a specially crafted request, an authenticated attacker could exploit this vulnerability to gain elevated privileges. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Data Protect versions 1.0.0 - 2.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7165476

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has issued the security update for the month of August addressing multiple vulnerabilities that exists in variety of Microsoft products, features, and roles. Updates include defense-in-depth updates to help strengthen security-related aspects, in addition to security improvements for the vulnerabilities. Microsoft strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	Microsoft .NET 8.0 App Installer Azure Connected Machine Agent Azure CycleCloud 8.0.0 Azure CycleCloud 8.0.1 Azure CycleCloud 8.0.2 Azure CycleCloud 8.1.0 Azure CycleCloud 8.1.1 Azure CycleCloud 8.2.0 Azure CycleCloud 8.2.1 Azure CycleCloud 8.2.2 Azure CycleCloud 8.3.0 Azure CycleCloud 8.4.0 Azure CycleCloud 8.4.1 Azure CycleCloud 8.4.2 Azure CycleCloud 8.5.0 Azure CycleCloud 8.6.0 Azure CycleCloud 8.6.1 Azure CycleCloud 8.6.2 Azure Health Bot Azure IoT Hub Device Client SDK Azure Linux 3.0 ARM Azure Linux 3.0 x64 Azure Stack Hub C SDK for Azure IoT CBL Mariner 1.0 ARM CBL Mariner 1.0 x64 CBL Mariner 2.0 ARM CBL Mariner 2.0 x64 Dynamics CRM Service Portal Web Resource Microsoft 365 Apps for Enterprise for 32-bit Systems Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Copilot Studio Microsoft Dynamics 365 (on-premises) version 9.1 Microsoft Edge (Chromium-based) Microsoft Office 2016 (32-bit edition) Microsoft Office 2016 (64-bit edition) Microsoft Office 2019 for 32-bit editions Microsoft Office 2019 for 64-bit editions Microsoft Office LTSC 2021 for 32-bit editions Microsoft Office LTSC 2021 for 64-bit editions Microsoft Office LTSC for Mac 2021 Microsoft OfficePLUS Microsoft Outlook 2016 (32-bit edition) Microsoft Outlook 2016 (64-bit edition) Microsoft PowerPoint 2016 (32-bit edition) Microsoft PowerPoint 2016 (64-bit edition) Microsoft Project 2016 (32-bit edition) Microsoft Project 2016 (64-bit edition) Microsoft Teams for iOS Microsoft Visual Studio 2022 version 17.10 Microsoft Visual Studio 2022 version 17.6 Microsoft Visual Studio 2022 version 17.8 Remote Desktop client for Windows Desktop Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for x64-based Systems 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 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows 11 Version 24H2 for ARM64-based Systems Windows 11 Version 24H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Aug

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41730, CVE-2024-29415)
Description	SAP has issued the security update for the month of August addressing multiple vulnerabilities that exists in variety of SAP products. **CVE-2024-41730 -** In SAP BusinessObjects Business Intelligence Platform, if Single Signed On is enabled on Enterprise authentication, an unauthorized user can get a logon token using a REST endpoint. The attacker can fully compromise the system resulting in High impact on confidentiality, integrity and availability. **CVE-2024-29415 -** The ip package through 2.0.1 for Node.js might allow SSRF because some IP addresses (such as 127.1, 01200034567, 012.1.2.3, 000:0:0000::01, and ::fFFf:127.0.0.1) are improperly categorized as globally routable via isPublic. NOTE: this issue exists because of an incomplete fix for CVE-2023-42282. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP BusinessObjects Business Intelligence Platform, Version – ENTERPRISE 430, 440 SAP Build Apps, Versions prior to 4.11.130
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use After Free, NULL Pointer Dereference, Out of Bounds Read. Red Hat 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://access.redhat.com/errata/RHSA-2024:5266 • https://access.redhat.com/errata/RHSA-2024:5266 • https://access.redhat.com/errata/RHSA-2024:5240 • https://access.redhat.com/errata/RHSA-2024:5239 • https://access.redhat.com/errata/RHSA-2024:5281 • https://access.redhat.com/errata/RHSA-2024:5282 • https://access.redhat.com/errata/RHSA-2024:5363 • https://access.redhat.com/errata/RHSA-2024:5364 • https://access.redhat.com/errata/RHSA-2024:5365

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38652, CVE-2024-38653, CVE-2024-36136, CVE-2024-37399, CVE-2024-37373, CVE-2024-7570)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Use After Free, Remote code Execution, NULL Pointer Dereference. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Avalanche - Versions 6.3.1 - 6.3.4, 6.4.0 - 6.4.3 Ivanti Neurons for ITSM - 2023.2, 2023.3, 2023.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Avalanche-6-4-4-CVE-2024-38652-CVE-2024-38653-CVE-2024-36136-CVE-2024-37399-CVE-2024-37373?language=en_US • https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Neurons-for-ITSM-CVE-2024-7569-CVE-2024-7570?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information Disclosure, memory corruption, Use-after-free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5, 15.6 openSUSE Leap Micro 5.5 Public Cloud Module 15-SP6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 12 SP5, 15 SP5 SUSE Linux Enterprise Server 11 SP4, 12 SP5, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE 11-SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5, 15 SP6 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242892-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242893-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242894-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242895-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242896-1/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39283, CVE-2024-22374, CVE-2024-24853, CVE-2021-26344, CVE-2021-26387, CVE-2021-46746, CVE-2021-46772, CVE-2023-20518, CVE-2023-20578, CVE-2023-20584, CVE-2023-20591, CVE-2023-31356)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Information Disclosure, Arbitrary Code Execution, Privilege Escalation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110 - Prior to v2.20_05-27-2024 HPE Alletra 4120 - Prior to v2.20_05-27-2024 HPE Alletra 4140 - Prior to v2.20_05-27-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.20_08-07-2024 HPE Compute Edge Server e930t - Prior to v2.20_05-27-2024 HPE Edgeline e920 Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920d Server Blade - Prior to v2.20_08-07-2024 HPE Edgeline e920t Server Blade - Prior to v2.20_08-07-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.20_08-07-2024 HPE ProLiant DL110 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DL20 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL320 Gen11 Server - Prior to v2.10_11-28-2023 HPE ProLiant DL320 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL325 Gen10 Plus server - Prior to v2.84_08-17-2023 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v2.84_08-17-2023 HPE ProLiant DL325 Gen10 Server - Prior to v2.84_09-07-2023 HPE ProLiant DL325 Gen11 Server - Prior to v1.58_01-04-2024 HPE ProLiant DL345 Gen10 Plus server - Prior to v2.84_08-17-2023 HPE ProLiant DL345 Gen11 Server - Prior to v1.58_01-04-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.10_11-28-2023 HPE ProLiant DL360 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL365 Gen10 Plus server - Prior to v2.84_08-17-2023 HPE ProLiant DL365 Gen11 Server - Prior to v1.58_01-04-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.20_08-07-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.10_11-28-2023 HPE ProLiant DL380 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant DL380a Gen11 - Prior to v2.10_11-28-2023 HPE ProLiant DL380a Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant DL385 Gen10 Plus server - Prior to v2.84_08-17-2023 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v2.84_08-17-2023 HPE ProLiant DL385 Gen10 Server - Prior to v2.84_09-07-2023 HPE ProLiant DL385 Gen11 Server - Prior to v1.58_01-04-2024 HPE ProLiant DL560 Gen11 - Prior to v2.10_11-28-2023 HPE ProLiant DL560 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.20_08-07-2024 HPE ProLiant ML110 Gen11 - Prior to v2.10_11-28-2023 HPE ProLiant ML110 Gen11 - Prior to v2.20_05-27-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v3.40_08-01-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.10_11-28-2023 HPE ProLiant ML350 Gen11 Server - Prior to v2.20_05-27-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.20_08-07-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.20_08-07-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.10_11-28-2023 HPE Synergy 480 Gen11 Compute Module - Prior to v2.20_05-27-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04680en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04677en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04681en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04684en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26344, CVE-2021-26387, CVE-2021-46772, CVE-2021-46746, CVE-2023-20518, CVE-2023-20578, CVE-2023-20584, CVE-2023-20591, CVE-2023-31356, CVE-2024-21981, CVE-2024-24853, CVE-2024-24980, CVE-2024-21801, CVE-2024-22374, CVE-2024-21810, CVE-2024-23497, CVE-2024-23981, CVE-2024-24986, CVE-2024-21807, CVE-2024-21769, CVE-2024-24983, CVE-2024-23499, CVE-2024-21806, CVE-2024-22376)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to compromise the affected systems. 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/000227760/dsa-2024-350-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227762/dsa-2024-308-security-update-for-dell-poweredge-server-for-intel-august-2024-security-advisories-2024-3-ipu • https://www.dell.com/support/kbdoc/en-us/000227763/dsa-2024-359-dell-poweredge-server-security-update-for-intel-ethernet-controllers-adapters-and-tdx-software-vulnerabilities

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42374, CVE-2023-30533, CVE-2024-34688, CVE-2024-33003, CVE-2024-39593, CVE-2023-0215, CVE-2022-0778 , CVE-2023-0286, CVE-2024-34683, CVE-2024-42376, CVE-2024-33005, CVE-2024-39594, CVE-2024-37176, CVE-2024-41735, CVE-2024-41733, CVE-2024-41737, CVE-2024-34689, CVE-2024-41732, CVE-2023-0023, CVE-2024-42375, CVE-2024-41736, CVE-2024-39591, CVE-2024-42373, CVE-2024-41734, CVE-2024-37180)
Description	SAP has issued the security update for the month of August addressing multiple vulnerabilities that exists in variety of SAP products. Exploitation of these vulnerabilities could lead to Denial of service, Cross-Site Scripting, Information Disclosure, Server-Side Request Forgery (SSRF) SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• SAP BEx Web Java Runtime Export Web Service, Versions - BI-BASE-E 7.5, BI-BASE-B 7.5, BI-IBC 7.5, BI-BASE-S 7.5, BIWEBAPP 7.5 • SAP S/4 HANA, Library Versions - SheetJS CE < 0.19.3 • SAP NetWeaver AS Java, Version – MMR_SERVER 7.5 • SAP Commerce Cloud, Versions – HY_COM 1808, 1811, 1905, 2005, 2105, 2011, 2205, COM_CLOUD 2211 • SAP Landscape Management, Version - VCM 3.00 • SAP Replication Server, Versions – 16.0.3, 16.0.4 • SAP Document Builder, Versions – S4CORE 100, 101, S4FND 102, 103, 104, 105, 106, 107, 108, SAP_BS_FND 702, 731, 746, 747, 748 • SAP Shared Service Framework, Versions – SAP_BS_FND 702, 731, 746, 747, 748 • SAP NetWeaver Application Server (ABAP and Java), SAP Web Dispatcher and SAP Content Server, Versions – KRNL64NUC 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT, 7.53, WEBDISP 7.53, 7.77, 7.85, 7.22_EXT, 7.89, 7.54, 7.93, KERNEL 7.22, 7.53, 7.77, 7.85, 7.89, 7.54, 7.93 • SAP Business Warehouse - Business Planning and Simulation, Versions – SAP_BW 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 758, SAP_BW_VIRTUAL_COMP 701 • SAP BW/4HANA Transformation and Data Transfer Process, Versions – DW4CORE 200, 300, 400, 796, SAP_BW 740, 750, 751, 752, 753, 754, 755, 756, 757, 758 • SAP Commerce Backoffice, Version – HY_COM 2205 • SAP Commerce, Versions – HY_COM 2205, COM_CLOUD 2211 • SAP CRM ABAP (Insights Management), Versions – BBPCRM 700, 701, 702, 712, 713, 714 • SAP Business Workflow (WebFlow Services), Versions – SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758 • SAP NetWeaver Application Server ABAP, Versions – SAP_UI 754, 755, 756, 757, 758, SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 912 • SAP Bank Account Management (Manage Banks), Versions – 800, 900 • SAP BusinessObjects Business Intelligence Platform, Versions – ENTERPRISE 420, 430, 440 • SAP Permit to Work, Versions – UIS4HOP1 800, 900 • SAP Document Builder, Versions – S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, S4FND 108, SAP_BS_FND 702, SAP_BS_FND 731, SAP_BS_FND 746, SAP_BS_FND 747, SAP_BS_FND 748 • SAP Document Builder, Versions – S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, S4FND 108, SAP_BS_FND 702, SAP_BS_FND 731, SAP_BS_FND 746, SAP_BS_FND 747, SAP_BS_FND 748 • SAP NetWeaver Application Server ABAP and ABAP Platform, Versions – SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 912 • SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions – SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/august-2024.html

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21147, CVE-2024-21140, CVE-2024-21144, CVE-2024-27267, CVE-2024-35136, CVE-2024-30172, CVE-2024-29857, CVE-2024-30171, CVE-2024-37529, CVE-2024-35152, CVE-2024-31882)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere and Db2 products. Exploitation of these vulnerabilities may lead to Denial of Service, Information Disclosure, Integrity, confidentiality and availability impacts. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server versions 8.5 and 9.0 IBM WebSphere Application Server Liberty Continuous Delivery versions IBM Db2 versions 10.5.0 - 10.5.11, 11.1.4 - 11.1.4.7 and 11.5.0 - 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7165423 • https://www.ibm.com/support/pages/node/7165341 • https://www.ibm.com/support/pages/node/7165342 • https://www.ibm.com/support/pages/node/7165340 • https://www.ibm.com/support/pages/node/7165343 • https://www.ibm.com/support/pages/node/7165338

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Server-Side Request Forgery (CVE-2024-39573)
Description	F5 has released security updates addressing Server-Side Request Forgery that exist in their products. **CVE-2024-39573 -** Potential SSRF in mod_rewrite in Apache HTTP Server 2.4.59 and earlier allows an attacker to cause unsafe RewriteRules to unexpectedly setup URL's to be handled by mod_proxy. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) - 17.1.0 - 17.1.1, 16.1.0 - 16.1.5, 15.1.0 - 15.1.10 F5OS-A - Versions 1.7.0, 1.5.1 - 1.5.2 F5OS-C - Versions 1.6.0 - 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000140693

Affected Product	**Fortiguard**	
Severity	**Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26211, CVE-2024-36505, CVE-2024-21757, CVE-2022-27486, CVE-2022-45862)	
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Execute unauthorized code or commands, Improper access control and Escalation of privileges. Fortiguard advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	FortiAnalyzer 7.0 7.0.0 through 7.0.10 FortiAnalyzer 7.2 7.2.0 through 7.2.4 FortiAnalyzer 7.4 7.4.0 through 7.4.1 FortiDDoS 4.5 -5.5 all versions FortiDDoS 5.6.0 through 5.6.1 FortiDDoS 5.7.0 FortiDDoS-F 6.1 - 6.3 all versions FortiDDoS-F 6.4.0 through 6.4.1 FortiDDoS-F 6.5.0 FortiManager 7.0.0 through 7.0.10 FortiManager 7.2.0 through 7.2.4 FortiManager 7.4.0 through 7.4.1	FortiOS 6.4 all versions FortiOS 7.0.12 through 7.0.14 FortiOS 7.0 all versions FortiOS 7.2.5 through 7.2.7 FortiOS 7.2.0 through 7.2.5 FortiOS 7.4.0 through 7.4.3 FortiPAM 1.0 – 1.3 all versions FortiProxy 7.0 – 7.2 all versions FortiSOAR 7.3.0 through 7.3.2 FortiSOAR 7.4.0 FortiSwitchManager 7.0 all versions FortiSwitchManager 7.2.0 through 7.2.1
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	• https://www.fortiguard.com/psirt/FG-IR-23-088 • https://www.fortiguard.com/psirt/FG-IR-24-012 • https://www.fortiguard.com/psirt/FG-IR-23-467 • https://www.fortiguard.com/psirt/FG-IR-22-047 • https://www.fortiguard.com/psirt/FG-IR-22-445	

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.