Advisory Alert

Alert Number: **AAA20231115** **Date:** **November 15, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Intel	**Critical**	Privilege escalation vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Redhat	**High, Medium**	Multiple Vulnerabilities
Intel	**High, Medium, Low**	Multiple Vulnerabilities
FortiGuard	**High, Medium, Low**	Multiple Vulnerabilities
HPE	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**High, Low**	Multiple Vulnerabilities
SAP	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-36049, CVE-2023-36560, CVE-2023-36038, CVE-2023-36558, CVE-2023-36052, CVE-2023-38151, CVE-2023-36021, CVE-2023-36437, CVE-2020-1747, CVE-2023-46316, CVE-2023-46753, CVE-2020-8554, CVE-2020-14343, CVE-2023-24023, CVE-2023-36016, CVE-2023-36007, CVE-2023-36031, CVE-2023-36410, CVE-2023-36030, CVE-2023-36014, CVE-2023-5996, CVE-2023-36022, CVE-2023-36027, CVE-2023-36029, CVE-2023-5480, CVE-2023-5856, CVE-2023-5855, CVE-2023-5854, CVE-2023-5859, CVE-2023-5858, CVE-2023-5857, CVE-2023-5850, CVE-2023-5849, CVE-2023-5482, CVE-2023-5853, CVE-2023-5852, CVE-2023-5851, CVE-2023-36024, CVE-2023-36034, CVE-2023-36439, CVE-2023-36050, CVE-2023-36039, CVE-2023-36035, CVE-2023-36413, CVE-2023-36045, CVE-2023-36041, CVE-2023-36037, CVE-2023-38177, CVE-2023-36423, CVE-2023-36401, CVE-2023-36402, CVE-2023-36394, CVE-2023-36719, CVE-2023-36043, CVE-2023-36393, CVE-2023-36042, CVE-2023-36018, CVE-2023-36047, CVE-2023-36428, CVE-2023-36046, CVE-2023-36036, CVE-2023-36424, CVE-2023-36396, CVE-2023-36422, CVE-2023-36395, CVE-2023-36392, CVE-2023-36425, CVE-2023-36033, CVE-2023-36400, CVE-2023-36427, CVE-2023-36407, CVE-2023-36406, CVE-2023-36408, CVE-2023-36705, CVE-2023-36397, CVE-2023-36405, CVE-2023-36404, CVE-2023-36403, CVE-2023-36398, CVE-2023-36028, CVE-2023-36017, CVE-2023-36025, CVE-2023-36399)
Description	Microsoft has released critical security updates for November 2023. This release includes fixes for several vulnerabilities across various Microsoft products. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	.NET Framework ASP.NET Azure Azure DevOps Mariner Microsoft Bluetooth Driver Microsoft Dynamics Microsoft Dynamics 365 Sales Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Office Microsoft Office Excel Microsoft Office SharePoint Microsoft Remote Registry Service Microsoft WDAC OLE DB provider for SQL Microsoft Windows Search Component Microsoft Windows Speech Open Management Infrastructure Tablet Windows User Interface Visual Studio Visual Studio Code Windows Authentication Methods Windows Cloud Files Mini Filter Driver Windows Common Log File System Driver Windows Compressed Folder Windows Defender Windows Deployment Services Windows DHCP Server Windows Distributed File System (DFS) Windows DWM Core Library Windows HMAC Key Derivation Windows Hyper-V Windows Installer Windows Internet Connection Sharing (ICS) Windows Kernel Windows NTFS Windows Protected EAP (PEAP) Windows Scripting Windows SmartScreen Windows Storage
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Nov

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-36553, CVE-2023-34991)
Description	Fortiguard has released critical security updates for FortiSIEM and FortiWLM. **CVE-2023-36553-** An improper neutralization of special elements used in in FortiSIEM report server may allow a remote unauthenticated attacker to execute unauthorized commands via crafted API requests. **CVE-2023-34991-** An improper neutralization of special elements used in sql command in FortiWLM may allow a remote unauthenticated attacker to execute unauthorized sql queries via a crafted http request. Fortiguard highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiSIEM 5.4 all versions FortiSIEM 5.3 all versions FortiSIEM 5.2 all versions FortiSIEM 5.1 all versions FortiSIEM 5.0 all versions FortiSIEM 4.10 all versions FortiSIEM 4.9 all versions FortiSIEM 4.7 all versions FortiWLM version 8.6.6 and below FortiWLM version 8.5.5 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-142 https://www.fortiguard.com/psirt/FG-IR-23-135

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40309, CVE-2023-31403)
Description	SAP has released a security update addressing multiple vulnerabilities which could lead to Privilege escalation and unauthorized file read and write. **CVE-2023-40309-** Privilege escalation vulnerability due to not performing necessary authentication checks in SAP CommonCryptoLib, which may result in missing or wrong authorization checks for an authenticated user. Depending on the application and the level of privileges acquired, an attacker could abuse functionality restricted to a particular user group as well as read, modify, or delete restricted data. **CVE-2023-31403 –** Vulnerability in SAP Business One installation - version 10.0, does not perform proper authentication and authorization checks for SMB shared folder. As a result, any malicious user can read and write to the SMB shared folder. Additionally, the files in the folder can be executed or be used by the installation process leading to considerable impact on confidentiality, integrity and availability. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP CommonCryptoLib, Version–8 SAP NetWeaver AS ABAP, SAP NetWeaver AS Java, and ABAP Platform of S/4HANA on-premise, Versions -KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.22, KERNEL 8.04, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64UC 8.04, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT SAP Web Dispatcher, Versions -7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 SAP Content Server, Versions -6.50, 7.53, 7.54 SAP HANA Database, Version–2.0 SAP Host Agent, Version–722 SAP Extended Application Services and Runtime (XSA), Versions -SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 SAP SSOEXT, Version–17 SAP Business One, Version –10.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**Intel**
Severity	**Critical**
Affected Vulnerability	Privilege escalation vulnerability (CVE-2023-31273)
Description	Intel has released security updates addressing Privilege escalation vulnerability that exists due to Protection mechanism failure in some Intel DCM software.by exploiting unauthenticated user could be able to privilege escalation via network access. Intel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Intel Data Center Manager software before version 5.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00902.html

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45614, CVE-2023-45615, CVE-2023-45616, CVE-2023-45617, CVE-2023-45618, CVE-2023-45619, CVE-2023-45620, CVE-2023-45621, CVE-2023-45622, CVE-2023-45623, CVE-2023-45624, CVE-2023-45625, CVE-2023-45626, CVE-2023-45627)
Description	HPE has released a security update addressing multiple vulnerabilities in Aruba access points. By exploiting, these vulnerabilities could lead to Compromise of System Integrity, Arbitrary Code Execution, Arbitrary Command Execution and Denial of Service HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Aruba access points running InstantOS and ArubaOS 10 • ArubaOS 10.5.x.x: 10.5.0.0 and below • ArubaOS 10.4.x.x: 10.4.0.2 and below • InstantOS 8.11.x.x: 8.11.1.2 and below • InstantOS 8.10.x.x: 8.10.0.8 and below • InstantOS 8.6.x.x: 8.6.0.22 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04565en_us

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-43975, CVE-2022-3594, CVE-2022-3640, CVE-2022-4744, CVE-2022-28388, CVE-2022-38457, CVE-2022-40133, CVE-2022-40982, CVE-2022-42895, CVE-2022-45869, CVE-2022-45887, CVE-2023-0458, CVE-2023-0590, CVE-2023-0597, CVE-2023-1073, CVE-2023-1074, CVE-2023-1075, CVE-2023-1079, CVE-2023-1118, CVE-2023-1206, CVE-2023-1252, CVE-2023-1382, CVE-2023-1855, CVE-2023-1989, CVE-2023-1998, CVE-2023-2513, CVE-2023-3141, CVE-2023-3161, CVE-2023-3212, CVE-2023-3268, CVE-2023-3609, CVE-2023-3611, CVE-2023-3772, CVE-2023-4128, CVE-2023-4132, CVE-2023-4155, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4732, CVE-2023-23455, CVE-2023-26545, CVE-2023-28328, CVE-2023-28772, CVE-2023-30456, CVE-2023-31084, CVE-2023-31436, CVE-2023-33203, CVE-2023-33951, CVE-2023-33952, CVE-2023-35823, CVE-2023-35824, CVE-2023-35825, CVE-2023-1393, CVE-2021-3750, CVE-2023-3301, CVE-2023-20569, CVE-2023-2602, CVE-2023-2603, CVE-2023-4527, CVE-2023-4806, CVE-2023-4813, CVE-2023-4911, CVE-2023-22652, CVE-2023-28484, CVE-2023-29469, CVE-2023-30079, CVE-2023-38545, CVE-2023-38546, CVE-2023-44487)
Description	Red Hat has released several important security updates to address multiple vulnerabilities in various products. It is strongly recommended to apply these updates to your systems to ensure the security and integrity of your Red Hat environment.
Affected Products	Kernel Module Management 1 for RHEL 9 x86_64 Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 8 s390x Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:7218 https://access.redhat.com/errata/RHSA-2023:7109 https://access.redhat.com/errata/RHSA-2023:7077 https://access.redhat.com/errata/RHSA-2023:6980 https://access.redhat.com/errata/RHSA-2023:6916 https://access.redhat.com/errata/RHSA-2023:6901

Affected Product	**Intel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has released several important security updates to address multiple vulnerabilities in their products. Exploitation of the most severe vulnerabilities could lead Escalation of Privilege, Information Disclosure and Denial of Service It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/default.html

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29177,CVE-2023-25603,CVE-2023-26205,CVE-2022-40681,CVE-2023-41840,CVE-2023-33304,CVE-2023-44248,CVE-2023-45582,CVE-2023-36633,CVE-2023-40719,CVE-2023-36641,CVE-2023-28002,CVE-2023-45585,CVE-2023-41676,CVE-2023-44252,CVE-2023-38545,CVE-2023-42783,CVE-2023-44251)
Description	Fortiguard has released several important security updates to address multiple vulnerabilities in fortiguard products. This release includes fixes for privilege escalation, denial of service, Arbitrary file deletion, Improper access control, bypass system protections. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	FGT_VM64_KVM version 7.0.1 through 7.0.13 FGT_VM64_KVM version 7.2.0 through 7.2.6 FGT_VM64_KVM version 7.4.0 through 7.4.1 FortiADC 5.2 all versions FortiADC 5.3 all versions FortiADC 5.4 all versions FortiADC 6.0 all versions FortiADC 6.1 all versions FortiADC 6.2 all versions FortiADC 7.0 all versions FortiADC 7.1 7.1.0 through 7.1.2 FortiADC 7.2 7.2.0 FortiAnalyzer 7.0 all versions FortiAnalyzer 7.2 7.2.0 through 7.2.3 FortiAnalyzer 7.4 7.4.0 FortiClientWindows 6.0 FortiClientWindows 6.2 FortiClientWindows 6.4 FortiClientWindows 7.0 FortiClientWindows 7.2 FortiClientWindows version 7.0.0 through 7.0.9 FortiDDoS-F 6.1 FortiDDoS-F 6.2 FortiDDoS-F 6.3 FortiDDoS-F 6.4 FortiDDoS-F 6.5 FortiEDRCollectorWindows 4.0 all versions FortiEDRCollectorWindows 5.0.3.1007 and below FortiEDRCollectorWindows version 5.2.0.4549 and below FortiMail 6.0 all versions FortiMail 6.2 all versions FortiMail 6.4 all versions FortiMail 7.0 7.0.0 through 7.0.6 FortiMail 7.2 7.2.0 through 7.2.4 FortiMail 7.4 7.4.0 FortiManager 7.0 7.0 all versions FortiManager 7.2 7.2.0 through 7.2.3 FortiManager 7.4 7.4.0 FortiOS 6.0 all versions FortiOS 6.2 all versions FortiOS 6.4 all versions FortiOS 7.0 through 7.0.12 FortiOS 7.2.0 through 7.2.5 FortiOS version 7.4.0 FortiProxy 1.0 all versions FortiProxy 1.1 all versions FortiProxy 1.2 all versions FortiProxy 2.0 all versions FortiProxy 7.0 all versions FortiProxy 7.2 all versions FortiSIEM 5.3 all versions FortiSIEM 5.4 all versions FortiSIEM 6.1 all versions FortiSIEM 6.2 all versions FortiSIEM 6.3 all versions FortiSIEM version 6.4.0 through 6.4.2 FortiSIEM version 6.5.0 through 6.5.1 FortiSIEM version 6.6.0 through 6.6.3 FortiSIEM version 6.7.0 through 6.7.5 FortiSIEM version 6.7.0 through 6.7.6 FortiSIEM version 7.0.0 FortiWAN version 5.1.1 through 5.1.2 FortiWAN version 5.2.0 through 5.2.1 FortiWLM version 8.6.0 through 8.6.6 FortiWLM version 8.5.0 through 8.5.4 FortiWLM 8.4 all versions FortiWLM 8.3 all versions FortiWLM 8.2 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-064 https://www.fortiguard.com/psirt/FG-IR-22-518 https://www.fortiguard.com/psirt/FG-IR-22-292 https://www.fortiguard.com/psirt/FG-IR-22-299 https://www.fortiguard.com/psirt/FG-IR-23-274 https://www.fortiguard.com/psirt/FG-IR-23-108 https://www.fortiguard.com/psirt/FG-IR-23-287 https://www.fortiguard.com/psirt/FG-IR-23-203 https://www.fortiguard.com/psirt/FG-IR-23-151 https://www.fortiguard.com/psirt/FG-IR-22-396 https://www.fortiguard.com/psirt/FG-IR-23-061 https://www.fortiguard.com/psirt/FG-IR-23-290 https://www.fortiguard.com/psirt/FG-IR-23-392 https://www.fortiguard.com/psirt/FG-IR-23-177 https://www.fortiguard.com/psirt/FG-IR-23-306 https://www.fortiguard.com/psirt/FG-IR-23-265 https://www.fortiguard.com/psirt/FG-IR-23-143 https://www.fortiguard.com/psirt/FG-IR-23-385

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23908, CVE-2022-40982, CVE-2022-41804, CVE-2023-23583, CVE-2022-23820, CVE-2021-46774, CVE-2023-20533, CVE-2023-20519, CVE-2023-20566, CVE-2023-20521, CVE-2021-46766, CVE-2022-23830, CVE-2023-20526, CVE-2021-26345)
Description	HPE has released security updates addressing multiple vulnerabilities in their products. By exploiting, these vulnerabilities could lead Arbitrary Code Execution, Denial of Service, Disclosure of Information, privilege escalation, Buffer Overflow. HPE recommended to apply necessary fixes at earliest to avoid issues
Affected Products	HPE Cray EX235n Server - Prior to 1.3.1 (HFP 23.9) HPE Cray EX425 Compute Blade - Prior to 1.7.2 (HFP 23.9) - Gen 2, and Gen 3 EPYC Processors. HPE Cray EX4252 Compute Blade - Prior to 1.4.0 (HFP 23.8) HPE ProLiant DL110 Gen10 Plus Telco server - Prior to 1.90_10-19-2023 HPE ProLiant DL20 Gen10 Plus server - Prior to 1.90_10-19-2023 HPE ProLiant DL325 Gen10 Plus server - Prior to 2.84 (HFP 23.9) HPE ProLiant DL325 Gen10 Plus server - Prior to 2.84_08-17-2023 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to 2.84_08-17-2023 HPE ProLiant DL325 Gen10 Server - Prior to 2.84_09-07-2023 HPE ProLiant DL325 Gen11 Server - Prior to v1.40_07-12-2023 HPE ProLiant DL345 Gen10 Plus server - Prior to 2.84_08-17-2023 HPE ProLiant DL345 Gen11 Server - Prior to v1.40_07-12-2023 HPE ProLiant DL360 Gen10 Plus server - Prior to 1.90_10-19-2023 HPE ProLiant DL365 Gen10 Plus server - Prior to 2.84_08-17-2023 HPE ProLiant DL365 Gen11 Server - Prior to v1.40_07-12-2023 HPE ProLiant DL380 Gen10 Plus server - Prior to 1.90_10-19-2023 HPE ProLiant DL385 Gen10 Plus server - Prior to 2.84 (HFP 23.9) HPE ProLiant DL385 Gen10 Plus server - Prior to 2.84_08-17-2023 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to 2.84_08-17-2023 HPE ProLiant DL385 Gen10 Server - Prior to 2.84_09-07-2023 HPE ProLiant DL385 Gen11 Server - Prior to v1.40_07-12-2023 HPE ProLiant DX385 Gen10 Plus server - Prior to 2.84_08-17-2023 HPE ProLiant DX385 Gen10 Plus v2 server - Prior to 2.84_08-17-2023 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to 1.90_10-19-2023 HPE ProLiant ML30 Gen10 Plus server - Prior to 1.90_10-19-2023 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to 2.84_08-17-2023 HPE ProLiant XL645d Gen10 Plus Server - Prior to 2.84 (HFP 23.9) HPE ProLiant XL645d Gen10 Plus Server - Prior to 2.84_08-17-2023 HPE ProLiant XL675d Gen10 Plus Server - Prior to 2.84 (HFP 23.9) HPE ProLiant XL675d Gen10 Plus Server - Prior to 2.84_08-17-2023 HPE SimpliVity 170r Gen10 Server - Prior to HPE OmniStack Firmware Version 2023_0913 HPE SimpliVity 190r Gen10 Server - Prior to HPE OmniStack Firmware Version 2023_0913 HPE SimpliVity 380 Gen10 - Prior to HPE OmniStack Firmware Version 2023_0913 HPE SimpliVity 380 Gen10 G - Prior to HPE OmniStack Firmware Version 2023_0913 HPE SimpliVity 380 Gen10 H - Prior to HPE OmniStack Firmware Version 2023_0913 HPE SimpliVity 380 Gen10 Plus - Prior to HPE OmniStack Firmware Version 2023_0913
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04562en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04561en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04563en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04559en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbcr04553en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04552en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04550en_us

Affected Product	**IBM**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22045, CVE-2023-22049, CVE-2023-2828, CVE-2023-24329, CVE-2022-4839)
Description	IBM has released several important security updates to address multiple vulnerabilities in their products. . Exploitation of the most severe vulnerabilities could lead bypass security restrictions, arbitrary commands execution, Denial of Service It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	IBM QRadar Network Packet Capture 7.5.0 IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5 IBM WebSphere Application Server Liberty Continuous delivery
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7028350 https://www.ibm.com/support/pages/node/7073360

Affected Product	**SAP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42477, CVE-2023-41366, CVE-2023-42480)
Description	SAP has released a security update addressing multiple vulnerabilities. Exploitation of the most severe vulnerabilities could lead to information discloser, Cross-Site Request Forgery and Server-Side Request Forgery SAP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP NetWeaver AS Java, Version –7.50 SAP SQL Anywhere, Versions –16.0, 17.0 SAP IQ, Version –16.0 SAP ASE, Versions –15.7, 16.0 SAP ASE Cluster Edition, Version –15.7 SAP Event Stream Processor, Version –5.1 SAP Replication Server, Version –15.7 SAP NetWeaver Application Server ABAP and ABAP Platform, Versions –KERNEL 722, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KERNEL 7.94, KERNEL64UC 7.22, KERNEL64UC 7.22EXT, KERNEL64UC 7.53, KERNEL64NUC 7.22, KERNEL64NUC 7.22EXT
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

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.