Public

SAP Security Patch Day – December 2023

THE BEST RUN SAP

OBJECTIVE :

This post shares information on Security Notes that remediate vulnerabilities discovered in SAP products. SAP strongly recommends that the customer visits the Support Portal and applies patches on priority to protect their SAP landscape.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit here.

SAP is committed to delivering trustworthy products and cloud services. Secure configuration is essential to ensuring secure operation and data integrity. We have therefore documented security recommendations that are consolidated in this document to help you configure the best security for your SAP portfolio.

Archived blogs from previous years are available here.

If you have any comments or feedback about this post, you can write to secure@sap.com.

DECEMBER 2023

On 12th of December 2023, SAP Security Patch Day saw the release of 15 new Security Notes. Further, there were 2 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3411067	**[Multiple CVEs] Escalation of Privileges in SAP Business Technology Platform (BTP) Security Services Integration Libraries** CVEs - CVE-2023-49583, CVE-2023-50422, CVE-2023-50423, CVE-2023-50424 Library- @sap/xssec, Versions – < 3.6.0 Library- cloud-security-services-integration-library, Versions – < 2.17.0 & from 3.0.0 before 3.3.0 Library- sap-xssec, Versions – < 4.1.0 Library- github.com/sap/cloud-security-client-go, Versions - < 0.17.0	Hot News	9.1
3399691	**Update 1 to 3350297 - [CVE-2023-36922] OS command injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL)** Product - SAP ECC and SAP S/4HANA (IS-OIL), Versions - 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807	Hot News	9.1
3350297	***Update to Security Note released on July 2023 Patch Day:*** [CVE-2023-36922] **OS command injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL)** Product - SAP ECC and SAP S/4HANA (IS-OIL), Versions - 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807	Hot News	9.1
3394567	**[CVE-2023-42481] Improper Access Control vulnerability in SAP Commerce Cloud** Product - SAP Commerce Cloud, Version – 8.1	High	8.1
3382353	**[CVE-2023-42478] Cross site scripting vulnerability in SAP BusinessObjects Business Intelligence Platform** Product - Business Objects BI Platform, Versions – 420, 430	High	7.5
3385711	**[CVE-2023-49580] Information disclosure vulnerability in SAP GUI for WIndows and SAP GUI for Java** Product - SAP GUI for Windows and SAP GUI for Java, Versions – SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758	High	7.3

3406244	[CVE-2023-6542] **Missing Authorization Check in SAP EMARSYS SDK ANDROID** Product - SAP EMARSYS SDK ANDROID, Version – 3.6.2	High	7.1
3369353	[CVE-2023-42476] **Cross Site Scripting vulnerability in SAP BusinessObjects Web Intelligence** Product - SAP BusinessObjects Web Intelligence , Version – 420	Medium	6.8
3395306	[CVE-2023-49587] **Command Injection vulnerability in SAP Solution Manager** Product - SAP Solution Manager, Version – 720	Medium	6.4
3383321	[CVE-2023-42479] **Cross-Site Scripting (XSS) vulnerability in SAP Biller Direct** Product - SAP Biller Direct, Versions – 635, 750	Medium	6.1
3217087	[CVE-2023-49577] **Cross-Site Scripting (XSS) vulnerability in the SAP HCM (SMART PAYE solution)** Product - SAP HCM (SMART PAYE solution), Versions – S4HCMCIE 100, SAP_HRCIE 600, SAP_HRCIE 604, SAP_HRCIE 608	Medium	6.1
3159329	**Denial of service (DoS) vulnerability in JSZip library bundled within SAPUI5** Related CVEs- CVE-2021-23413 Product – SAPUI5, Versions – SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756, UI_700 200	Medium	5.3
3406786	[CVE-2023-49584] **Client-Side Desynchronization vulnerability in SAP Fiori Launchpad** Product - SAP Fiori Launchpad, Versions – SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, UI_700 200, SAP_BASIS 793	Medium	4.3
3392547	[CVE-2023-49581] **SQL Injection vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform** Product - SAP NetWeaver Application Server ABAP and ABAP Platform, Versions – SAP_BASIS 700, SAP_BASIS731, SAP_BASIS740, SAP_BASIS750	Medium	4.1
3363690	[CVE-2023-49058] **Directory Traversal vulnerability in SAP Master Data Governance** Product - SAP Master Data Governance, Versions – 731, 732, 746, 747, 748, 749, 800, 751, 752, 801, 802, 803, 804, 805, 806, 807, 808 Product - SAP_BS_FND, Version – 702	Low	3.5
3362463	[CVE-2023-49578] **Denial of service (DOS) in SAP Cloud Connector** Product - SAP Cloud Connector, Version – 2.0	Low	3.5

NOVEMBER 2023

On 14th of November 2023, SAP Security Patch Day saw the release of 3 new Security Notes. Further, there were 3 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
3340576	***Update to Security Note released on September 2023 Patch Day:*** **[CVE-2023-40309] Missing Authorization check in SAP CommonCryptoLib** Product - SAP CommonCryptoLib, Versions – 8 Product - 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 Product – SAP Web Dispatcher, Versions - 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 Product – SAP Content Server, Versions - 6.50, 7.53, 7.54 Product – SAP HANA Database, Versions – 2.0 Product – SAP Host Agent, Versions – 722 Product - SAP Extended Application Services and Runtime (XSA), Versions - SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 Product – SAPSSOEXT, Versions – 17	Hot News	9.8
3355658	**[CVE-2023-31403] Improper Access Control vulnerability in SAP Business One product installation** Product - SAP Business One, Version – 10.0	Hot News	9.6
3333426	***Update to Security Note released on October 2023 Patch Day:*** **[CVE-2023-42477] Server-Side Request Forgery in SAP NetWeaver AS Java (GRMG Heartbeat application)** Product - SAP NetWeaver AS Java, Version – 7.50	Medium	6.5
2494184	***Update to Security Note released on August 2017 Patch Day:*** **Cross-Site Request Forgery (CSRF) vulnerability in multiple SAP Sybase products** Product - SAP SQL Anywhere, Version – 16.0, 17.0 Product - SAP IQ, Version – 16.0 Product - SAP ASE, Version – 15.7, 16.0 Product - SAP ASE Cluster Edition, Version – 15.7 Product - SAP Event Stream Processor, Version – 5.1 Product - SAP Replication Server, Version – 15.7	Medium	6.3
3362849	**[CVE-2023-41366] Information Disclosure vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform** Product - SAP NetWeaver Application Server ABAP and ABAP Platform, Version – 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	Medium	5.3
3366410	**[CVE-2023-42480] Information Disclosure in NetWeaver AS Java Logon** Product - NetWeaver AS Java, Version – 7.50	Medium	5.3

OCTOBER 2023

On 10th of October 2023, SAP Security Patch Day saw the release of 7 new Security Notes. Further, there were 2 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3372991	**[**CVE-2023-42474**] Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Web Intelligence** Product - SAP BusinessObjects Web Intelligence, Versions – 420	Medium	6.8
3357154	**[**CVE-2023-40310**] Missing XML Validation vulnerability in SAP PowerDesigner Client (BPMN2 import)** Product – SAP PowerDesigner Client, Version – 16.7	Medium	6.5
3333426	**[**CVE-2023-42477**] Server-Side Request Forgery in SAP NetWeaver AS Java (GRMG Heartbeat application)** Product - SAP NetWeaver AS Java, Version – 7.50	Medium	6.5
3219846	**[**CVE-2023-42473**] Missing Authorization Check In S/4HANA (Manage Withholding Tax Items)** Product -S/4HANA (Manage Withholding Tax Items), Version – 106	Medium	5.4
3371873	**Update 1 to Security Note 3324732: [**CVE-2023-31405**] Log Injection vulnerability in SAP NetWeaver AS for Java (Log Viewer)** Product - Product - SAP NetWeaver AS for Java (Log Viewer), Version - ENGINEAPI 7.50	Medium	5.3
3324732	***Update to Security Note released on July 2023 Patch Day:*** **[**CVE-2023-31405**] Log Injection vulnerability in SAP NetWeaver AS for Java (Log Viewer)** Product - SAP NetWeaver AS for Java (Log Viewer), Version - ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50	Medium	5.3
3338380	**[**CVE-2023-41365**] Information Disclosure vulnerability in SAP Business One (B1i)** Product - SAP Business One (B1i), Version – 10	Medium	4.3
3222121	**[**CVE-2023-42475**] Information Disclosure Vulnerability in Statutory Reporting** Product - SAP S/4HANA Core, Version – S4CORE 102, S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, SAPSCORE 128	Medium	4.3

SEPTEMBER 2023

On 12th of September 2023, SAP Security Patch Day saw the release of 13 new Security Notes. Further, there was 5 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3320355	[CVE-2023-40622] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Promotion Management)** Product - SAP BusinessObjects Business Intelligence Platform (Promotion Management), Versions – 420,430	Hot News	9.9
3273480	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41272] **Improper access control in SAP NetWeaver AS Java (User Defined Search)** Product – SAP NetWeaver Process Integration, Version – 7.50	Hot News	9.9

3245526	***Update to Security Note released on March 2023 Patch Day:*** [CVE-2023-25616] **Code Injection vulnerability in SAP Business Objects Business Intelligence Platform (CMC)** Product - SAP Business Objects Business Intelligence Platform (CMC), Versions – 420, 430	Hot News	9.9
3340576	[CVE-2023-40309] **Missing Authorization check in SAP CommonCryptoLib** Product - SAP CommonCryptoLib, Versions – 8 Product - 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 Product – SAP Web Dispatcher, Versions - 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 Product – SAP Content Server, Versions - 6.50, 7.53, 7.54 Product – SAP HANA Database, Versions – 2.0 Product – SAP Host Agent, Versions – 722 Product - SAP Extended Application Services and Runtime (XSA), Versions - SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 Product – SAPSSOEXT, Versions – 17	Hot News	9.8
3370490	[CVE-2023-42472] **Insufficient File type validation in SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface)** Product - SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface), Versions – 420	High	8.7
3327896	[CVE-2023-40308] **Memory Corruption vulnerability in SAP CommonCryptoLib** Product - SAP CommonCryptoLib, Versions – 8 Product - 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 Product – SAP Web Dispatcher, Versions - 7.22EXT, 7.53, 7.54, 7.77, 7.85, 7.89 Product – SAP Content Server, Versions - 6.50, 7.53, 7.54 Product – SAP HANA Database, Versions – 2.0 Product – SAP Host Agent, Versions – 722 Product - SAP Extended Application Services and Runtime (XSA), Versions - SAP_EXTENDED_APP_SERVICES 1, XS_ADVANCED_RUNTIME 1.00 Product – SAPSSOEXT, Versions – 17	High	7.5
3357163	[CVE-2023-40621] **Code Injection vulnerability in SAP PowerDesigner Client** Product - SAP PowerDesigner Client, Version – 16.7	Medium	6.3
3317702	[CVE-2023-40623] **Arbitrary File Delete via Directory Junction in SAP BusinessObjects Suite(installer)** Product - SAP BusinessObjects Suite (Installer), Version – 420, 430	Medium	6.2
3156972	***Update to Security Note released on August 2023 Patch Day:*** [CVE-2023-40306] **URL Redirection vulnerability in SAP S/4HANA (Manage Catalog Items and Cross-Catalog search)** Product - SAP S/4HANA (Manage Catalog Items and Cross-Catalog search), Versions – S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106	Medium	6.1
3149794	***Update to Security Note released on August 2023 Patch Day:*** **Cross-Site Scripting (XSS) vulnerabilities in jQuery-UI library bundled with SAPUI5** Related CVEs- CVE-2021-41184, CVE-2021-41183, CVE-2021-41182, Product – SAPUI5, Versions – SAP_UI 750, SAP_UI 753, SAP_UI 754, SAP_UI 755, SAP_UI 756, UI_700 200	Medium	6.1

3349805	**Denial of service (DOS) vulnerability due to the usage of vulnerable version of Commons FileUpload in SAP Quotation Management Insurance (FS-QUO)** Related CVE - CVE-2023-24998 Product - SAP Quotation Management Insurance (FS-QUO), Versions – 400, 510, 700, 800	Medium	5.7
3323163	[CVE-2023-40624] **Code Injection vulnerability in SAP NetWeaver AS ABAP (applications based on Unified Rendering)** Product - SAP NetWeaver AS ABAP (applications based on Unified Rendering), Versions – SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, SAP_UI 758, SAP_BASIS 702, SAP_BASIS 731	Medium	5.5
3326361	[CVE-2023-40625] **Missing Authorization check in S4CORE (Manage Purchase Contracts App)** Product - S4CORE (Manage Purchase Contracts App), Versions – 102, 103, 104, 105, 106, 107	Medium	5.4
3352453	[CVE-2023-37489] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Version Management System)** Product - SAP BusinessObjects Business Intelligence Platform (Version Management System), Versions – 430	Medium	5.3
3348142	[CVE-2023-41367] **Missing Authentication check in SAP NetWeaver (Guided Procedures)** Product - SAP NetWeaver (Guided Procedures), Version – 7.50	Medium	5.3
3369680	[CVE-2023-41369] **External Entity Loop vulnerability in SAP S/4HANA (Create Single Payment application)** Product - SAP S/4HANA (Create Single Payment application), Versions – 100, 101, 102, 103, 104, 105, 106, 107, 108	Low	3.5
3355675	[CVE-2023-41368] **Insecure Direct Object Reference (IDOR) vulnerability in SAP S/4HANA (Manage checkbook apps)** Product - S4 HANA ABAP (Manage checkbook apps), Versions – 102, 103, 104, 105, 106, 107	Low	2.7

AUGUST 2023

On 8th of August 2023, SAP Security Patch Day saw the release of 15 new Security Notes. Further, there was 3 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
3341460	[CVE-2023-37483] **Multiple Vulnerabilities in SAP PowerDesigner** Additional CVE - CVE-2023-37484 Product - SAP PowerDesigner, Version – 16.7	Hot News	9.8
3350297	***Update to Security Note released on July 2023 Patch Day:*** [CVE-2023-36922] **OS command injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL)** Product - SAP ECC and SAP S/4HANA (IS-OIL), Versions - 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807	Hot News	9.1
3346500	[CVE-2023-39439] **Improper authentication in SAP Commerce Cloud** Product - SAP Commerce, Versions – HY_COM 2105, HY_COM 2205, COM_CLOUD 2211	High	8.8
3331376	***Update to Security Note released on July 2023 Patch Day:*** [CVE-2023-33989] **Directory Traversal vulnerability in SAP NetWeaver (BI CONT ADD ON)** Product - SAP NetWeaver (BI CONT ADD ON), Versions – 707, 737, 747, 757	High	8.7

3341599	[CVE-2023-36923] **Code Injection vulnerability in SAP PowerDesigner** Product - SAP PowerDesigner, Version – 16.7	High	7.8
3358300	[CVE-2023-39437] **Cross-Site Scripting (XSS) vulnerability in SAP Business One** Product - SAP Business One, Version – 10.0	High	7.6
3317710	[CVE-2023-37490] **Binary hijack in SAP BusinessObjects Business Intelligence Suite (installer)** Product - SAP BusinessObjects Business Intelligence (installer), Versions – 420, 430	High	7.6
3312047	**Denial of Service (DoS) vulnerability due to the usage of vulnerable version of Commons FileUpload in SAP BusinessObjects Business Intelligence Platform (CMC)** Product - SAP BusinessObjects Business Intelligence Platform, Versions – 420	High	7.5
3344295	[CVE-2023-37491] **Improper Authorization check vulnerability in SAP Message Server** Product - SAP Message Server, Versions – KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EX	High	7.5
3337797	[CVE-2023-33993] **SQL Injection vulnerability in SAP Business One (B1i Layer)** Product - SAP Business One (B1i Layer), Version – 10.0	High	7.1
2032723	***Update to Security Note released on November 2014 Patch Day:*** **Switchable authorization checks for RFC in SRM** Product - SAP Supplier Relationship Management, Versions – 600, 602, 603, 604, 605, 606, 616, 617	Medium	6.3
3350494	[CVE-2023-37488] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Process Integration** Product - SAP NetWeaver Process Integration, Versions - SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50	Medium	6.1
3341934	[CVE-2023-37486] **Information Disclosure vulnerability in SAP Commerce (OCC API)** Product - SAP Commerce (OCC API), Versions - HY_COM 2105, HY_COM 2205, COM_CLOUD 2211	Medium	5.9
2067220	[CVE-2023-39436] **Information Disclosure in SAP Supplier Relationship Management** Product - SAP Supplier Relationship Management, Versions – 600, 602, 603, 604, 605, 606, 616, 617	Medium	5.8
3333616	[CVE-2023-37487] **Security Misconfiguration vulnerability in SAP Business One (Service Layer)** Product - SAP Business One (Service Layer), Version – 10.0	Medium	5.3
3348000	[CVE-2023-37492] **Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS 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 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804	Medium	4.9
3312586	[CVE-2023-39440] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions – 430	Medium	4.4
3358328	[CVE-2023-36926] **Information disclosure vulnerability in SAP Host Agent** Product – SAP Host Agent, Version – 7.22	Low	3.7

JULY 2023

On 11th of July 2023, SAP Security Patch Day saw the release of 16 new Security Notes. Further, there was 2 updates to previously released Security Note.

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3350297	[CVE-2023-36922] **OS command injection vulnerability in SAP ECC and SAP S/4HANA (IS-OIL)** Product - SAP ECC and SAP S/4HANA (IS-OIL), Versions - 600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807	Hot News	9.1
3331376	[CVE-2023-33989] **Directory Traversal vulnerability in SAP NetWeaver (BI CONT ADD ON)** Product - SAP NetWeaver (BI CONT ADD ON), Versions – 707, 737, 747, 757	High	8.7
3233899	[CVE-2023-33987] **Request smuggling and request concatenation vulnerability in SAP Web Dispatcher** Product - SAP Web Dispatcher, Versions – WEBDISP 7.49, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85, WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1	High	8.6
3324285	***Update to Security Note released on June 2023 Patch Day:*** [CVE-2023-33991] **Stored Cross-Site Scripting vulnerability in SAP UI5 (Variant Management)** Product - SAP UI5 Variant Management, Versions – SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200	High	8.2
3331029	[CVE-2023-33990] **Denial of service (DOS) vulnerability in SAP SQL Anywhere** Product - SAP SQL Anywhere, Version - 17.0	High	7.8
3340735	[CVE-2023-35871] **Memory Corruption vulnerability in SAP Web Dispatcher** Product - SAP Web Dispatcher, Versions - WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP 7.89, WEBDISP 7.91, WEBDISP 7.92, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1	High	7.7
3352058	[CVE-2023-36925] **Unauthenticated blind SSRF in SAP Solution Manager (Diagnostics agent)** Product - SAP Solution Manager (Diagnostic Agent), Versions – 7.20	High	7.2
3348145	[CVE-2023-36921] **Header Injection in SAP Solution Manager (Diagnostic Agent)** Product - SAP Solution Manager (Diagnostic Agent), Versions – 7.20	High	7.2
3343547	[CVE-2023-35873] **Missing Authentication check in SAP NetWeaver Process Integration (Runtime Workbench)** Product – SAP NetWeaver Process Integration (Runtime Workbench), Versions – SAP_XITOOL 7.50	Medium	6.5

3343564	[CVE-2023-35872] **Missing Authentication check in SAP NetWeaver Process Integration (Message Display Tool)** Product – SAP NetWeaver Process Integration (Message Display Tool), Versions – SAP_XIAF 7.50	Medium	6.5
3341211	[CVE-2023-35870] **Improper Access Control in SAP S/4HANA (Manage Journal Entry Template)** Product - SAP S/4HANA (Manage Journal Entry Template), Versions – S4CORE 104, 105, 106, 107	Medium	6.3
3326769	[**Multiple CVEs**] **Multiple Vulnerabilities in SAP Enable Now** CVEs - CVE-2023-33988, CVE-2023-36918, CVE-2023-36920, CVE-2023-36919 Product - SAP Enable Now, Version - WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704	Medium	6.1
3318850	[CVE-2023-35874] **Improper authentication vulnerability in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Version - KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL 7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93	Medium	6.0
3320702	[CVE-2023-36917] **Password Change rate limit bypass in SAP BusinessObjects Business Intelligence Platform** Product - SAP BusinessObjects BI Platform (Enterprise), Version - 4.20, 430	Medium	5.9
3324732	[CVE-2023-31405] **Log Injection vulnerability in SAP NetWeaver AS for Java (Log Viewer)** Product - SAP NetWeaver AS for Java (Log Viewer), Version - ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50	Medium	5.3
3351410	[CVE-2023-36924] **Log Injection vulnerability in SAP ERP Defense Forces and Public Security** Product - SAP ERP Defense Forces and Public Security, Version - 600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807	Medium	4.9
3088078	[CVE-2023-33992] **Missing Authorization Check in SAP Business Warehouse and SAP BW/4HANA** Product - SAP Business Warehouse and SAP BW/4HANA, Version - SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300	Medium	4.5

JUNE 2023

On 13th of June 2023, SAP Security Patch Day saw the release of 8 new Security Notes. Further, there was 5 updates to previously released Security Note.

Note#	Title	Priority	CVSS
3102769	***Update to Security Note released on December 2021 Patch Day:*** [CVE-2021-42063] **Cross-Site Scripting (XSS) vulnerability in SAP Knowledge Warehouse** Product - SAP Knowledge Warehouse, Versions - 7.30, 7.31, 7.40, 7.50	High	8.8
3324285	[CVE-2023-33991] **Stored Cross-Site Scripting (Stored XSS) vulnerability in UI5 Variant Management** Product - SAP UI5 Variant Management, Versions – SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200	High	8.2

3301942	[CVE-2023-2827] **Missing Authentication in SAP Plant Connectivity and Production Connector for SAP Digital Manufacturing** Product - SAP Plant Connectivity, Version – 15.5	High	7.9
3326210	***Update to Security Note released on May 2023 Patch Day:*** [CVE-2023-30743] **Improper Neutralization of Input in SAPUI5** Product - SAPUI5, Versions – SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200	High	7.1
3142092	***Update to Security Note released on February 2022 Patch Day:*** [CVE-2022-22542] **Information Disclosure vulnerability in SAP S/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer)** Product - SAP S/4HANA (Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer), Versions - 104, 105, 106	Medium	6.5
3318657	[CVE-2023-33984] **Cross-Site Scripting (XSS) vulnerability in NetWeaver (Design Time Repository)** Product - SAP NetWeaver (Design Time Repository), Versions - 7.50	Medium	6.4
3331627	[CVE-2023-33985] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions – 7.50	Medium	6.1
2826092	[CVE-2023-33986] **Cross-Site Scripting (XSS) vulnerability in SAP CRM ABAP (Grantor Management)** Product - SAP CRM ABAP (Grantor Management), Versions – 430	Medium	6.1
3322800	**Update 1 to security note 3315971 - [CVE-2023-30742] Cross-Site Scripting (XSS) vulnerability in SAP CRM (WebClient UI)** Product – SAP CRM (WebClient UI), Versions – S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 80	Medium	6.1
3315971	***Update to Security Note released on May 2023 Patch Day:*** [CVE-2023-30742] **Cross-Site Scripting (XSS) vulnerability in SAP CRM (WebClient UI)** Product – SAP CRM (WebClient UI), Versions – S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 80	Medium	6.1
3319400	***Update to Security Note released on May 2023 Patch Day:*** [CVE-2023-31406] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions – 420, 430	Medium	6.1
1794761	[CVE-2023-32115] **SQL Injection in Master Data Synchronization (MDS COMPARE TOOL)** Product - Master Data Synchronization (MDS COMPARE TOOL), Version - SAP_APPL 600, 602, 603, 604, 605, 606, 616	Medium	4.2
3325642	[CVE-2023-32114] **Denial of Service in SAP NetWeaver (Change and Transport System)** Product - SAP NetWeaver (Change and Transport System), Version - 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Low	2.7

MAY 2023

On 9th of May 2023, SAP Security Patch Day saw the release of 18 new Security Notes. Further, there was 5 updates to previously released Security Note.

Note#	Title	Priority	CVSS
3328495	**Multiple vulnerabilities associated with Reprise License Manager 14.2 component used with SAP 3D Visual Enterprise License Manager** Related CVEs - CVE-2021-44151,CVE-2021-44152,CVE-2021-44153, CVE-2021-44154,CVE-2021-44155 Product - SAP 3D Visual Enterprise License Manager, Version – 15	Hot News	9.8
3307833	[CVE-2023-28762] **Information Disclosure vulnerabilities in SAP BusinessObjects Intelligence Platform** Product - SAP BusinessObjects Intelligence Platform, Versions – 420, 430	Hot News	9.1
3317453	[CVE-2023-30744] **Improper access control during application start-up in SAP AS NetWeaver JAVA** Product - SAP AS NetWeaver JAVA, Versions - SERVERCORE 7.50, J2EE-FRMW 7.50, CORE-TOOLS 7.50	High	8.2
3323415	[CVE-2023-29080] **Privilege escalation vulnerability in SAP IBP add-in for Microsoft Excel** Product – SAP IBP EXCEL ADD-IN, Versions – 2211, 2302, 2305	High	8.2
3213507	***Update to Security Note released on August 2022 Patch Day:*** [CVE-2022-31596] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (CMC)** Product - SAP BusinessObjects Intelligence Platform, Versions – 430	High	8.2
3217303	***Update to Security Note released on September 2022 Patch Day:*** [CVE-2022-39014] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (CMC)** Product - SAP BusinessObjects Intelligence Platform, Versions – 430	High	7.7
3300624	[CVE-2023-32111] **Memory Corruption vulnerability in SAP PowerDesigner (Proxy)** Product - SAP PowerDesigner (Proxy), Version - 16.7	High	7.5
3320145	**Denial of service (DOS) in SAP Commerce** Related CVE - CVE-2022-41966 Product - SAP Commerce, Versions – 2105, 2205 Product - SAP Commerce, Version – 2211	High	7.5
3320467	[CVE-2023-32113] **Information Disclosure vulnerability in SAP GUI for Windows** Product - SAP GUI for Windows, Versions - 7.70, 8,0	High	7.5
3321309	**Information Disclosure vulnerability in SAP Commerce (Backoffice)** Related CVE - CVE-2023-32111 Product - **SAP Commerce (Backoffice),** Version – 2105, 2205	High	7.5
3326210	[CVE-2023-30743] **Improper Neutralization of Input in SAPUI5** Product - SAPUI5, Versions - SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 20	High	7.1
3233226	***Update to Security Note released on October 2022 Patch Day:*** [CVE-2022-32244] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Commentary DB)** Product - SAP BusinessObjects Intelligence Platform, Versions – 420, 430	Medium	6.8
3313484	[CVE-2023-30740] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	Medium	6.3
3309935	[CVE-2023-30741] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence platform** Product – SAP BusinessObjects Business Intelligence Platform, Versions – 420, 430	Medium	6.1

3315971	[CVE-2023-30742] **Cross-Site Scripting (XSS) vulnerability in SAP CRM (WebClient UI)** Product – SAP CRM (WebClient UI), Versions – S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 80	Medium	6.1
3319400	[CVE-2023-31406] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions – 420, 430	Medium	6.1
3213524	***Update to Security Note released on August 2022 Patch Day:*** [CVE-2022-32244] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Commentary DB)** Product - SAP BusinessObjects Intelligence Platform, Versions – 420, 430	Medium	6.0
3312892	[CVE-2023-31407] **Cross-Site Scripting (XSS) vulnerability in SAP Business Planning and Consolidation** Product – SAP Business Planning and Consolidation, Versions - 740, 750	Medium	5.4
3315979	[CVE-2023-29188] **Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI** Product - SAP CRM WebClient UI, Versions – SAPSCORE 129, S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 80	Medium	5.4
3145769	***Update to Security Note released on April 2022 Patch Day:*** [CVE-2022- 27667] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (CMC)** Product - SAP BusinessObjects Intelligence Platform, Versions – 430	Medium	5.3
3038911	[CVE-2023-31404] **Information Disclosure in SAP BusinessObjects Business Intelligence Platform (Central Management Service)** Product - SAP BusinessObjects Business Intelligence Platform (Central Management Service), Versions - 420, 430	Medium	5.0
3302595	[CVE-2023-28764] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence platform** Product - SAP BusinessObjects Platform, Versions – 420, 430	Low	3.7
3117978	***Update to Security Note released on April 2023 Patch Day:*** [CVE-2023-29111] **Information Disclosure vulnerability in SAP Application Interface Framework (ODATA service)** Product – SAP Application Interface Framework (ODATA service), Versions –755, 756	Low	3.1
2335198	[CVE-2023-32112] **Missing Authorization Check in Vendor Master Hierarchy** Product - Vendor Master Hierarchy, Versions – SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100	Low	2.8

APRIL 2023

On 11th of April 2023, SAP Security Patch Day saw the release of 18 new Security Notes. Further, there were 5 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
3305369	[CVE-2023-27497] **Multiple vulnerabilities in SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector)** Additional CVE - CVE-2023-27267 Product - SAP Diagnostics Agent (OSCommand Bridge and EventLogServiceCollector), Version – 720	Hot News	10.0
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3273480	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41272] **Improper access control in SAP NetWeaver AS Java (User Defined Search)** Product – SAP NetWeaver Process Integration, Version – 7.50	Hot News	9.9
3298961	[CVE-2023-28765] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Promotion Management)** Product - SAP BusinessObjects Business Intelligence Platform (Promotion Management, Versions – 420, 430	Hot News	9.8
3294595	***Update to Security Note released on March 2023 Patch Day*** [CVE-2023-27269] **Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791	Hot News	9.6
3305907	[CVE-2023-29186] **Directory Traversal vulnerability in SAP NetWeaver (BI CONT ADD ON)** Product - SAP NetWeaver (BI CONT ADDON), Versions - 707, 737, 747, 757	High	8.7
3312733	[CVE-2023-26458] **Information Disclosure vulnerability in SAP Landscape Management** Product – SAP Landscape Management, Version – 3.0	Medium	6.8
3311624	[CVE-2023-29187] **DLL Hijacking vulnerability in SapSetup (Software Installation Program)** Product – SapSetup (Software Installation Program), Version – 9.0	Medium	6.7
3289994	[CVE-2023-28761] **Missing Authentication check in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal ,Version – 7.50	Medium	6.5
3290901	***Update to Security Note released on February 2023 Patch Day:*** [CVE-2023-24528] **Missing Authorization Check in SAP Fiori apps for Travel Management in SAP ERP (My Travel Requests)** Product – SAP Fiori apps 1.0 for travel management in SAP ERP (My Travel Requests), Version - 600	Medium	6.5
3296378	[CVE-2023-28763] **Denial of Service in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver AS for ABAP and ABAP Platform, Versions – 740, 750, 751, 752, 753, 754, 755, 756, 757, 791	Medium	6.5
3275458	[CVE-2023-27499] **Cross-Site Scripting (XSS) vulnerability in SAP GUI for HTML** Product - SAP GUI for HTML, Versions - KERNEL 7.22, 7.53, 7.547.77, 7.81, 7.85, 7.89, 7.91, KRNL64UC, 7.22, 7.22EXT, KRNL64UC 7.22, 7.22EXT	Medium	6.1
3309056	[CVE-2023-27897] **Code Injection vulnerability in SAP CRM** Product - SAP CRM, Versions – 700, 701, 702, 712, 713	Medium	6.0
3269352	[CVE-2023-29189] **HTTP Verb Tampering vulnerability in SAP CRM WebClient UI**	Medium	5.4

	Product - SAP CRM (WebClient UI) ,Versions – S4FND 102, 103, 104, 105, 106, 107, WEBCUIF, 700, 701, 731, 730, 746, 747, 748, 800, 801		
3000663	***Update to Security Note released on July 2021 Patch Day:*** [CVE-2021-33683] **HTTP Request Smuggling in SAP Web Dispatcher and Internet Communication Manager** Product - SAP Web Dispatcher and Internet Communication Manager, Versions - KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.73, WEBDISP 7.53, 7.73, 7.77, 7.81, 7.82, 7.83, KERNEL 7.21, 7.22, 7.49, 7.53, 7.73, 7.77, 7.81, 7.82, 7.83	Medium	5.4
3287784	[CVE-2023-24527] **Improper Access Control in SAP NetWeaver AS Java for Deploy Service** Product - SAP NetWeaver AS Java for Deploy Service, Version – 7.50	Medium	5.3
3303060	[CVE-2023-29185] **Denial of Service (DOS) in SAP NetWeaver AS for ABAP (Business Server Pages)** Product - SAP NetWeaver AS for ABAP (Business Server Pages), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	5.3
3315312	[CVE-2023-29108] **IP filter vulnerability in ABAP Platform and SAP Web Dispatcher** Product - ABAP Platform and SAP Web Dispatcher ,Versions - WEBDISP 7.85, 7.89, KERNEL 7.85, 7.89, 7.91	Medium	5.0
3316509	**Remote Code Execution vulnerability in SAP Commerce** Related CVE - CVE-2020-13936 Product - SAP Commerce, Versions – 1905, 2005, 2011	Medium	4.7
3115598	[CVE-2023-29109] **Code Injection vulnerability in SAP Application Interface Framework (Log Message View of Message Dashboard)** Product – SAP Application Interface Framework (Log Message View of Message Dashboard), Versions – AIF 703, AIFX 702, S4CORE 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E	Medium	4.4
3301457	[CVE-2023-1903] **Missing Authorization check in SAP HCM Fiori App My Forms (Fiori 2.0)** Product – SAP HCM Fiori App My Forms (Fiori 2.0), Version – 605	Medium	4.3
3113349	[CVE-2023-29110] **Code Injection vulnerability in SAP Application Interface Framework (Custom Hint of Message Dashboard)** Product – SAP Application Interface Framework (Custom Hint of Message Dashboard Application, Versions – AIF 703, AIFX 702, S4CORE 100, 101, SAP_BASIS 755, 756, SAP_ABA 75C, 75D, 75E	Low	3.7
3114489	[CVE-2023-29112] **Code Injection vulnerability in SAP Application Interface Framework (Message Monitoring and Message Monitoring for Administrators Application)** Product - SAP Application Interface Framework (Message Monitoring and Message Monitoring for Administrators Application, Versions – 600, 700	Low	3.7
3117978	[CVE-2023-29111] **Information Disclosure vulnerability in SAP Application Interface Framework (ODATA service)** Product – SAP Application Interface Framework (ODATA service), Versions –755, 756	Low	3.1

MARCH 2023

On 14th of March 2023, SAP Security Patch Day saw the release of 19 new Security Notes. Further, there were 2 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
3245526	[CVE-2023-25616] **Code Injection vulnerability in SAP Business Objects Business Intelligence Platform (CMC)** Product - SAP Business Objects Business Intelligence Platform (CMC), Versions – 420, 430	Hot News	9.9
3252433	[CVE-2023-23857] **Improper Access Control in SAP NetWeaver AS for Java** Product - SAP NetWeaver AS for Java, Version – 7.50	Hot News	9.9
3273480	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41272] **Improper access control in SAP NetWeaver AS Java (User Defined Search)** Product – SAP NetWeaver Process Integration, Version – 7.50	Hot News	9.9
3294595	[CVE-2023-27269] **Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791	Hot News	9.6
3302162	[CVE-2023-27500] **Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform (SAPRSBRO Program)** Product – SAP NetWeaver AS for ABAP and ABAP Platform (SAPRSBRO Program), Versions – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Hot News	9.6
3283438	[CVE-2023-25617] **OS command execution vulnerability in SAP Business Objects Business Intelligence Platform (Adaptive Job Server)** Product – SAP Business Objects (Adaptive Job Server), Versions – 420, 430	Hot News	9.0
3296476	[CVE-2023-27893] **Arbitrary Code Execution in SAP Solution Manager and ABAP managed systems (ST-PI)** Product - SAP Solution Manager and ABAP managed systems(ST-PI), Versions - 2008_1_700, 2008_1_710 and 740	High	8.8
3294954	[CVE-2023-27501] **Directory Traversal vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver AS for ABAP and ABAP Platform, Versions – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791	High	8.7
3296346	[CVE-2023-26459] **Multiple vulnerabilities in SAP NetWeaver AS for ABAP and ABAP Platform** Additional CVE - CVE-2023-25618 Product - SAP NetWeaver AS for ABAP and ABAP Platform, Versions - SAP_BASIS 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791	High	7.4
3275727	[CVE-2023-27498] **Memory Corruption vulnerability in SAPOSCOL** Product - SAP Host Agent, Versions – 7.22	High	7.2
3284550	[CVE-2023-26461] **XXE vulnerability in SAP NetWeaver (SAP Enterprise Portal)** Product - SAP NetWeaver (SAP Enterprise Portal), Versions – 7.50	Medium	6.8
3289844	[CVE-2023-25615] **SQL Injection vulnerability in ABAP Platform** Product - SAP ABAP Platform, Versions - 751, 753, 753, 754, 756, 757, 791	Medium	6.8
3296328	[CVE-2023-27270] **Denial of Service (DoS) in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791	Medium	6.5
3287120	[Multiple CVEs] **Multiple vulnerabilities in the SAP BusinessObjects Business Intelligence platform**	Medium	6.5

	CVEs - CVE-2023-27271, CVE-2023-27896, CVE-2023-27894 Product - SAP BusinessObjects Business Intelligence Platform (Web Services), Versions – 420, 430		
3281484	[CVE-2023-26457] **Cross-Site Scripting (XSS) vulnerability in SAP Content Server** Product – SAP Content Server, Version – 7.53	Medium	6.1
3302710	[CVE-2023-27895] **Information Disclosure vulnerability in SAP Authenticator for Android** Product – SAP Authenticator for Android, Version – 1.3.0	Medium	6.1
3274920	[CVE-2023-0021] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver** Product – SAP NetWeaver, Versions – 700, 701, 702, 731, 740, 750	Medium	6.1
3274585	***Update to Security Note released on February 2023 Patch Day:*** [CVE-2023-25614] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP (BSP Framework)** Product - SAP NetWeaver AS ABAP (BSP Framework), Version – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3288480	[CVE-2023-27268] **Missing Authentication and Authorization check in SAP NetWeaver AS Java (Object Analyzing Service)** Product – SAP NetWeaver AS Java (Object Analyzing Service), Versions – 7.50	Medium	5.3
3288096	[CVE-2023-26460] **Missing Authentication check in SAP NetWeaver AS for Java (Cache Management Service)** Product – SAP NetWeaver AS Java, Versions – 7.50	Medium	5.3
3288394	[CVE-2023-24526] **Improper Access Control in SAP NetWeaver AS Java (Classload Service)** Product – SAP NetWeaver AS Java, Versions – 7.50	Medium	5.3

FEBRUARY 2023

On 14th of February 2023, SAP Security Patch Day saw the release of 21 new Security Notes. Further, there were 5 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on April 2018 Patch Day:*** **Security updates for the browser control Google Chromium delivered with SAP Business Client** Product - SAP Business Client, Versions - 6.5, 7.0, 7.70	Hot News	10.0
3285757	[CVE-2023-24523] **Privilege Escalation vulnerability in SAP Start Service** Product - SAP Host Agent Service, Versions - 7.21, 7.22	High	8.8

3268172	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41264] **Code Injection vulnerability in SAP BASIS** Product – SAP BASIS, Versions – 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, 791	High	8.8
3263135	[CVE-2023-0020] **Information disclosure vulnerability in SAP BusinessObjects Business Intelligence platform** Product - SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP), Versions - 420, 430	High	8.5
3271091	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41268] **Privilege escalation vulnerability in SAP Business Planning and Consolidation** Product - SAP Business Planning and Consolidation, Versions – SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, DWCORE 200, 300, CPMBPC 810	High	8.5
3256787	[CVE-2023-24530] **Unrestricted Upload of File in SAP BusinessObjects Business Intelligence Platform (CMC)** Product - SAP BusinessObjects Business Intelligence platform (CMC), Versions - 420, 430	High	8.4
3265846	[CVE-2023-0024] **Cross Site Scripting in SAP Solution Manager (BSP Application)** Product – SAP Solution Manager (BSP Application), Version – 720	Medium	6.5
3267442	[CVE-2023-0025] **Cross Site Scripting in SAP Solution Manager (BSP Application)** Product – SAP Solution Manager (BSP Application), Version – 720	Medium	6.5
3270509	[CVE-2023-23855] **URL Redirection vulnerability in SAP Solution Manager** Product – SAP Solution Manager, Version – 720	Medium	6.5
3281724	[CVE-2023-0019] **Missing Authorization check in GRC function modules** Product – SAP GRC Process Control application, Versions – GRCFND_A V1200, V8100, GRCPINW V1100_700, V1100_731, V1200_750	Medium	6.5
3290901	[CVE-2023-24528] **Missing Authorization Check in SAP Fiori apps for Travel Management in SAP ERP (My Travel Requests)** Product – SAP Fiori apps 1.0 for travel management in SAP ERP (My Travel Requests), Version - 600	Medium	6.5
2985905	[CVE-2023-24524] **Missing Authorization check in SAP S/4 HANA Map Treasury Correspondence Format Data** Product – SAP S/4 HANA (Map Treasury Correspondence Format Data), Versions - 104, 105	Medium	6.5
3266751	[CVE-2023-23852] **Cross-Site Scripting (XSS) vulnerability in SAP Solution Manager 7.2** Product – SAP Solution Manager, Version – 720	Medium	6.1
3268959	**[Multiple CVEs] Multiple vulnerabilities in SAP NetWeaver AS for ABAP and ABAP Platform** CVEs - CVE-2023-23859 , CVE-2023-23860 Product - SAP NetWeaver AS for ABAP and ABAP Platform, Version – 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790	Medium	6.1
3271227	[CVE-2023-23853] **URL Redirection vulnerability in SAP NetWeaver Application Server for ABAP and ABAP Platform** Product – SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions – 700, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790	Medium	6.1
3282663	[CVE-2023-24529] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP (Business Server Pages application)** Product - SAP NetWeaver AS ABAP (Business Server Pages application), Version – 700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H	Medium	6.1

3293786	[CVE-2023-23858] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver AS for ABAP and ABAP Platform, Versions – 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3262544	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41262] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS for Java (Http Provider Service)** Product - SAP NetWeaver AS for Java (Http Provider Service), Version – 7.50	Medium	6.1
3274585	[CVE-2023-25614] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP (BSP Framework)** Product - SAP NetWeaver AS ABAP (BSP Framework), Version – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3269151	[CVE-2023-24521] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP (BSP Framework)** Product - SAP NetWeaver AS ABAP (BSP Framework), Version – 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3269118	[CVE-2023-24522] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP (BSP Framework)** Product - SAP NetWeaver AS ABAP (BSP Framework), Version – 700, 701, 702, 731, 740	Medium	6.1
3283283	***Update to Security Note released on January 2023 Patch Day:*** [CVE-2023-0013] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver AS for ABAP and ABAP Platform, Version – 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3275841	[CVE-2023-23851] **Unrestricted File Upload in SAP Business Planning and Consolidation** Product - SAP Business Planning and Consolidation, Versions – 200, 300	Medium	5.4
3263863	[CVE-2023-23856] **Cross-Site Scripting (XSS) vulnerability in Web Intelligence Interface** Product - SAP BusinessObjects Business Intelligence (Web Intelligence UI, Version – 430	Medium	4.3
2788178	[CVE-2023-24525] **Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI** Product - SAP CRM (WebClient UI), Versions – 700, 701, 702, 731, 740, 750, 751, 752, WEBCUIF 748, 800, 801, S4FND 102, 103	Medium	4.3
3287291	[CVE-2023-23854] **Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions – 700, 701, 702, 731, 740, 750, 751, 752	Low	3.8

JANUARY 2023

On 10th of January 2023, SAP Security Patch Day saw the release of 9 new Security Notes. Further,there were 3 updates to previously released Security Notes.

Note#	Title	Priority	CVSS
3275391	[CVE-2023-0016] **SQL Injection vulnerability in SAP Business Planning and Consolidation MS** Product - SAP BPC MS 10.0, Versions - 800, 810	Hot News	9.9
3262810	[CVE-2023-0022] **Code Injection vulnerability in SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP)** Product - SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP), Versions - 420, 430	Hot News	9.9

3273480	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41272] **Improper access control in SAP NetWeaver Process Integration (User Defined Search)** Product – SAP NetWeaver Process Integration, Version – 7.50	Hot News	9.9
3243924	***Update to Security Note released on November 2022 Patch Day:*** [CVE-2022-41203] **Insecure Deserialization of Untrusted Data in SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad)** Product - SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad), Versions - 4.2, 4.3	Hot News	9.9
3267780	***Update to Security Note released on December 2022 Patch Day:*** [CVE-2022-41271] **Improper access control in SAP NetWeaver Process Integration (Messaging System)** Product - SAP NetWeaver Process Integration, Version – 7.50	Hot News	9.4
3268093	[CVE-2023-0017] **Improper access control in SAP NetWeaver AS for Java** Product – SAP NetWeaver AS for Java, Version – 7.50	Hot News	9.4
3089413	[CVE-2023-0014] **Capture-replay vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product – SAP NetWeaver ABAP Server and ABAP Platform, Versions - SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT	Hot News	9.0
3276120	[CVE-2023-0012] **Local Privilege Escalation in SAP Host Agent (Windows)** Product - SAP Host Agent (Windows), Versions - 7.21, 7.22	Medium	6.4
3283283	[CVE-2023-0013] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS for ABAP and ABAP Platform** Product - SAP NetWeaver AS for ABAP and ABAP Platform, Version – 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3266006	[CVE-2023-0018] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (Central management console)** Product – SAP BusinessObjects Business Intelligence Platform (Central management console), Versions – 420, 430	Medium	5.4
3251447	[CVE-2023-0015] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence (Web Intelligence)** Product - SAP BusinessObjects Business Intelligence Platform, Version – 420	Medium	4.6
3150704	[CVE-2023-0023] **Information Disclosure in SAP Bank Account Management (Manage Banks)** Product - SAP Bank Account Management (Manage Banks), Versions – 800, 900	Medium	4.5

www.sap.com/contactsap

THE BEST RUN SAP