Public

SAP Security Patch Day – December 2022

THE BEST RUN

OBJECTIVE :

This post shares information on Patch Day Security Notes* that are released on second Tuesday of every month and fix vulnerabilities discovered in SAP products. SAP strongly recommends that the customer visits the Support Portal and applies patches on a priority to protect their SAP landscape.

* Patch Day Security Notes are all notes that appear under the category of “Patch Day Notes” in SAP Support Portal

** Any Patch Day Security Note released after the second Tuesday, will be accounted for in the following SAP Security Patch Day.

Customers who would like to look at all Security Notes published or updated after a certain date, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between <date 1> - <date 2>' → Go.

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

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.

Do write to us at secure@sap.com with all your comments and feedback on this blog post.

DECEMBER 2022

On 13th of December 2022, SAP Security Patch Day saw the release of 14 new Patch Day Security Notes. Further, there were 5 updates to previously released Patch Day Security.

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
3239475	[CVE-2022-41267] **Server-Side Request Forgery vulnerability in SAP BusinessObjects Business Intelligence Platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	Hot News	9.9
3273480	[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
3271523	**Remote Code Execution vulnerability associated with Apache Commons Text in SAP Commerce** Related CVE - CVE-2022-42889 Product – SAP Commerce, Versions - 1905, 2005, 2105, 2011, 2205	Hot News	9.8
3267780	[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
3268172	[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
3271091	[CVE-2022-41268] **Privilege escalation vulnerability in SAP Business Planning and Consolidation**	High	8.5

	Product - SAP Business Planning and Consolidation, Versions – SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, DWCORE 200, 300, CPMBPC 810		
3229132	***Update to Security Note released on October 2022 Patch Day:*** [CVE-2022-39013] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Program Objects)** Product - SAP BusinessObjects Business Intelligence Platform (Program Objects) ,Versions - 420, 430	High	8.2
3248255	[CVE-2022-41266] **Cross-Site Scripting (XSS) vulnerability in SAP Commerce** Product - SAP Commerce Webservices 2.0 (Swagger UI), Versions - 1905, 2005, 2105, 2011, 2205	High	8.0
3249990	***Update to Security Note released on November 2022 Patch Day:*** **Multiple Vulnerabilities in SQlite bundled with SAPUI5** Related CVE **-** CVE-2022-35737 Product – SAPUI5 CLIENT RUNTIME, Versions – 600, 700, 800, 900, 1000 Product – SAPUI5, Versions – 754, 755, 756, 757	High	7.5
3266846	[CVE-2022-41274] **Missing Authorization Checks in SAP Disclosure Management** Product - SAP Disclosure Management, Version – 10.1	Medium	6.5
3262544	[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
3271313	[CVE-2022-41275] **Open Redirect in SAP Solutions Manager (Enterprise Search)** Product - SAP Solution Manager (Enterprise Search), Versions – 740, 750	Medium	6.1
2872782	***Update to Security Note released on April 2020 Patch Day:*** [CVE-2020-6215] **URL Redirection vulnerability in SAP NetWeaver AS ABAP – Business Server Pages Test Application IT00** Product - SAP NetWeaver AS ABAP (Business ServerPages Test Application IT00), Versions - 700, 701, 702,730, 731, 740, 750, 751, 752, 753, 754	Medium	6.1
3258950	**Update 1 to Security Note 2872782 -** [CVE-2020-6215] **URL Redirection vulnerability in SAP NetWeaver AS ABAP (BSP Test Application)** Product - SAP NetWeaver AS ABAP (Business Server Pages Test Application IT00), Versions - 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757	Medium	6.1
3265173	[CVE-2022-41261] **Improper Access Control in SAP Solution Manager (Diagnostic Agent)** Product - SAP Solution Manager (Diagnostic Agent), Version – 7.20	Medium	6.0
3251202	***Update to Security Note released on November 2022 Patch Day:*** [CVE-2022-41215] **URL Redirection vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver ABAP Server and ABAP Platform, Versions - 700-702, 731, 740, 750-757, 789, 790	Medium	4.7
3249648	[CVE-2022-41263] **Missing authentication check vulnerability in SAP Business Objects Business Intelligence Platform (Web intelligence)** Product -SAP Business Objects Business Intelligence Platform (Web intelligence), Versions - 420, 430	Medium	4.3
3270399	[CVE-2022-41273] **URL Redirection vulnerability in SAP Sourcing and SAP Contract Lifecycle Management** Product - SAP Sourcing and SAP Contract Lifecycle Management, Version - 1100	Medium	4.3

NOVEMBER 2022

On 8th of November 2022, SAP Security Patch Day saw the release of 9 new Patch Day Security Notes. Further, there were 2 updates to previously released Patch Day Security Notes and 1 update to Security note released on November Patch Day.

Note#	Title	Priority	CVSS
3243924	[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
3239152	***Update to Security Note released on October 2022 Patch Day:*** [CVE-2022-41204] **Account hijacking through URL Redirection vulnerability in SAP Commerce login form** Product – SAP Commerce, Versions - 1905, 2005, 2105, 2011, 2205	Hot News	9.6
3256571	[CVE-2022-41214] **Multiple vulnerabilities in SAP NetWeaver Application Server ABAP and ABAP Platform** Additional CVE- CVE-2022-41212 Product - SAP NetWeaver Application Server ABAP and ABAP Platform, Versions - 700, 731, 804, 740, 750, 789	High	8.7
3226411	***Update to Security Note released on July 2022 Patch Day:*** [CVE-2022-35291] **Privilege escalation vulnerability in SAP SuccessFactors attachment API for Mobile Application(Android & iOS)** Product - SAP SuccessFactors attachment API for Mobile Application(Android & iOS), Versions - <8.1.2	High	8.1
3249990	***Update to Security Note released on November 2022 Patch Day:*** **Multiple Vulnerabilities in SQlite bundled with SAPUI5** Related CVE **-** https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20223 CVE-2022-35737 Product – SAPUI5 CLIENT RUNTIME, Versions – 600, 700, 800, 900, 1000 Product – SAPUI5, Versions – 754, 755, 756, 757	High	7.5
3263436	[CVE-2022-41211] **Arbitrary Code Execution vulnerability in SAP 3D Visual Enterprise Author and SAP 3D Visual Enterprise Viewer** Product - SAP 3D Visual Enterprise Author, Version – 9.0 Product - SAP 3D Visual Enterprise Viewer, Version – 9.0	High	7.0
3229987	[CVE-2022-41259] **Denial of service (DOS) in SAP SQL Anywhere** Product - SAP SQL Anywhere, Version - 17.0	Medium	6.5
3260708	[CVE-2022-41258] **Multiple Cross-Site Scripting (XSS) vulnerabilities in SAP Financial Consolidation** Additional CVEs - CVE-2022-41260, CVE-2022-41208 Product - SAP Financial Consolidation, Version - 1010	Medium	6.5
3238042	[CVE-2022-41207] **URL Redirection vulnerability in SAP Biller Direct** Product - SAP Biller Direct, Versions - 635, 750	Medium	6.1
3237251	[CVE-2022-41205] **Code injection vulnerability in SAP GUI for Windows** Product - SAP GUI for Windows, Version – 7.70	Medium	5.5
3251202	[CVE-2022-41215] **URL Redirection vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver ABAP Server and ABAP Platform, Versions - 700-702, 731, 740, 750-757, 789, 790	Medium	4.7

OCTOBER 2022

On 11th of October 2022, SAP Security Patch Day saw the release of 15 new Patch Day Security Notes. Further, there were 2 updates to previously released Patch Day Security Notes.

Note#	Title	Priority	CVSS
3242933	[CVE-2022-39802] **File path traversal vulnerability in SAP Manufacturing Execution** Product - SAP Manufacturing Execution, Versions - 15.1, 15.2, 15.3	Hot News	9.9
3239152	[CVE-2022-41204] **Account hijacking through URL Redirection vulnerability in SAP Commerce login form** Product – SAP Commerce, Versions - 1905, 2005, 2105, 2011, 2205	Hot News	9.6
3229132	[CVE-2022-39013] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Program Objects)** Product - SAP BusinessObjects Business Intelligence Platform (Program Objects) ,Versions - 420, 430	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 (Monitoring DB)** Product - SAP Business Objects Platform (Monitoring DB), Version - 430	High	8.2
3232021	[CVE-2022-35299] **Buffer Overflow in SAP SQL Anywhere and SAP IQ** Product - SAP SQL Anywhere, Version - 17.0 Product - SAP IQ, Version - 16.1	High	8.1
3239293	[CVE-2022-39015] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (AdminTools/ Query Builder)** Product - SAP BusinessObjects Business Intelligence Platform (Admin Tools/Query Builder), Versions – 420, 430	High	7.7
3245928	[Multiple CVEs] **Multiple vulnerabilities in SAP 3D Visual Enterprise Viewer** CVEs – CVE-2022-41186, CVE-2022-41187, CVE-2022-41188, CVE-2022-41189, CVE-2022-41190, CVE-2022-41191, CVE-2022-41192, CVE-2022-41193, CVE-2022-41194, CVE-2022-41195, CVE-2022-41196, CVE-2022-41197, CVE-2022-41198, CVE-2022-41199, CVE-2022-41200, CVE-2022-41201, CVE-2022-41202 Product - SAP 3D Visual Enterprise Viewer, Version - 9	High	7.0
3245929	[Multiple CVEs] **Multiple vulnerabilities in SAP 3D Visual Enterprise Author** CVEs - CVE-2022-39803, CVE-2022-39804, CVE-2022-39805, CVE-2022-39806, CVE-2022-39807, CVE-2022-39808, CVE-2022-41166, CVE-2022-41167, CVE-2022-41168, CVE-2022-41169, CVE-2022-41170, CVE-2022-41171, CVE-2022-41172, CVE-2022-41173, CVE-2022-41174, CVE-2022-41175, CVE-2022-41176, CVE-2022-41177, CVE-2022-41178, CVE-2022-41179, CVE-2022-41180, CVE-2022-41181, CVE-2022-41182, CVE-2022-41183, CVE-2022-41184, CVE-2022-41185 Product - SAP 3D Visual Enterprise Author, Version - 9	High	7.0
3233226	[CVE-2022-35296] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Version Management System)** Product - SAP BusinessObjects Business Intelligence Platform (Version Management System), Versions – 420, 430	Medium	6.8
3049899	[CVE-2022-35297] **Stored Cross-Site Scripting (XSS) vulnerability in SAP Enable Now** Product - SAP Enable Now, Version - 10	Medium	6.5

3202523	**Cross-Site Scripting (XSS) vulnerability in SAP Commerce** Related CVE - CVE-2021-41184 Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011, 2205	Medium	6.1
3211161	[CVE-2022-39800] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (BI LaunchPad)** Product - SAP BusinessObjects Business Intelligence Platform (BI LaunchPad), 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 Business Intelligence Platform (Commentary DB), Versions - 420, 430	Medium	6.0
3229425	[CVE-2022-41206] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence platform / Analysis for OLAP** Product - SAP BusinessObjects Business Intelligence platform (Analysis for OLAP), Version - 420, 430	Medium	5.4
3248384	[CVE-2022-41210] **Information Disclosure Vulnerability in SAP Customer Data Cloud (Gigya)** Product - SAP Customer Data Cloud (Gigya), Versions – 7.4	Medium	4.9
3248970	[CVE-2022-41209] **Information Disclosure Vulnerability in SAP Customer Data Cloud (Gigya)** Product - SAP Customer Data Cloud (Gigya), Versions – 7.4	Medium	4.9
3167342	[CVE-2022-35226] **Cross-Site Scripting (XSS) vulnerability in Data Services Management Console** Product - SAP Data Services Management Console, Versions - 4.2, 4.3	Medium	4.8

SEPTEMBER 2022

On 13th of September 2022, SAP Security Patch Day saw the release of 8 new Security Notes. Further, there were 5 updates to previously released Patch Day 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
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
3226411	***Update to Security Note released on July 2022 Patch Day:*** [CVE-2022-35291] **Privilege escalation vulnerability in SAP SuccessFactors attachment API for Mobile Application(Android & iOS)** Product - SAP SuccessFactors attachment API for Mobile Application(Android & iOS), Versions - <8.0.5	High	8.1
3223392	[CVE-2022-35292] **Windows Unquoted Service Path issue in SAP Business One** Product - SAP Business One, Versions - 10.0	High	7.8
2998510	***Update to Security Note released on May 2022 Patch Day:*** [CVE-2022-28214] **Central Management Server Information Disclosure in Business Intelligence Update** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	High	7.8

3217303	[CVE-2022-39014] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (CMC)** Product - SAP BusinessObjects Business Intelligence Platform (CMC), Versions - 430	High	7.7
3237075	[CVE-2022-39801] **Insufficient Firefighter Session Expiration in SAP GRC Access Control Emergency Access Management** Product - SAP Access Control, Version - 12	High	7.1
3159736	[CVE-2022-35295] **Privilege Escalation Vulnerability in SAPOSCol on Unix** Product - SAP BusinessObjects Business Intelligence Platform (Version Management System), Versions - 420, 430	Medium	6.7
3219164	[CVE-2022-35298] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal (KMC)** Product - SAP NetWeaver Enterprise Portal (KMC), Version - 7.50	Medium	6.1
3229820	[CVE-2022-39799] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP (SAP GUI for HTML within the Fiori Launchpad)** Product - SAP NetWeaver AS ABAP (SAP GUI for HTML within the Fiori Launchpad), Version - KERNEL 7.77, 7.81, 7.85, 7.89, 7.54	Medium	6.1
3218177	[CVE-2022-35294] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server ABAP** Product - SAP NetWeaver AS ABAP, Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.89, 7.54	Medium	5.4
3198137	**Update 1 to Security Note 3165333 -** [CVE-2022-28215] **URL Redirection vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver ABAP Server and ABAP Platform, Versions - 700, 701, 702, 731, 740, 750-757, 789	Medium	4.7
3165333	***Update to Security Note released on April 2022 Patch Day:*** [CVE-2022-28215] **URL Redirection vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver ABAP Server and ABAP Platform, Versions - 740, 750-756, 787	Medium	4.7

AUGUST 2022

On 9th of August 2022, SAP Security Patch Day saw the release of 5 new Security Notes. Further, there were 2 updates to previously released Patch Day 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
3210823	[CVE-2022-32245] **Information disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Open Document)** Product - SAP BusinessObjects Business Intelligence Platform (Open Document), Versions - 420, 430	High	8.2
2245130	***Update to Security Note released on February 2016 Patch Day:*** **Potential bypass of unified connectivity runtime checks possible in BC-MID-RFC** Product - SAP NetWeaver, Versions - 740, 750	Medium	6.3

3216653	[CVE-2022-35290] **Information Disclosure in SAP Authenticator for Android** Product - SAP Authenticator for Android, Versions <1.2.17	Medium	5.3
3213507	[CVE-2022-31596] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Monitoring DB)** Product -SAP Business Objects Platform (Monitoring DB), Version - 430	Medium	5.2
3213524	[CVE-2022-32244] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Commentary DB)** Product - SAP BusinessObjects Business Intelligence Platform (Commentary DB), Versions - 420, 430	Medium	5.2
3210566	[CVE-2022-35293] **Missing authorization check in SAP Enable Now Manager** Product - SAP Enable Now Manager, Version - 1.0	Medium	4.2

JULY 2022 – OUT-OF-BAND RELEASE

Note#	Title	Priority	CVSS
3226411	[CVE-2022-35291] **Privilege escalation vulnerability in SAP SuccessFactors attachment API for Mobile Application (Android & iOS)** Product - SAP SuccessFactors Mobile Application (Android iOS), Version - 8.0.5	High	8.1

JULY 2022

On 12th of July 2022, SAP Security Patch Day saw the release of 20 new Security Notes. Further, there were 3 updates to previously released Patch Day Security Notes.

Note#	Title	Priority	CVSS
3221288	[CVE-2022-35228] **Information disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (Central management console)** Product - SAP BusinessObjects Business Intelligence Platform (Central management console), Versions - 420, 430	High	8.3
3212997	[CVE-2022-32249] **Information Disclosure vulnerability in SAP Business One** Product - SAP Business One, Version - 10.0	High	7.6
3157613	[CVE-2022-28771] **Missing Authentication check in SAP Business One (License service API)** Product - SAP Business One License service API, Version - 10.0	High	7.5
3191012	[CVE-2022-31593] **Code Injection vulnerability in SAP Business One** Product - SAP Business One, Version - 10.0	High	7.4
3169239	[CVE-2022-29619] **Information Disclosure to user Administrator in SAP BusinessObjects Business Intelligence Platform 4.x** Product - SAP BusinessObjects Business Intelligence Platform 4.x, Versions - 420, 430	Medium	6.5
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

3165801	***Update to Security Note released on May 2022 Patch Day:*** [CVE-2022-29611] **Missing Authorization check in SAP NetWeaver Application Server for ABAP and ABAP Platform** Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788	Medium	6.5
3207902	[CVE-2022-35172] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3208819	[CVE-2022-35170] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3208880	[CVE-2022-35225] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3209557	[CVE-2022-32247] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3210779	[CVE-2022-35224] **Cross-Site Scripting (XSS) vulnerability in SAP Enterprise Portal** Product - SAP Enterprise Portal, Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3211760	[CVE-2022-35227] **Cross-Site Scripting (XSS) vulnerability in SAP NW EP WPC** Product - SAP NetWeaver Enterprise Portal (WPC), Versions - 7.30, 7.31, 7.40, 7.50	Medium	6.1
3194361	[CVE-2022-35169] **Information Disclosure vulnerability in SAP BusinessObjects Business Intelligence Platform (LCM)** Product - SAP BusinessObjects Business Intelligence Platform (LCM), Versions - 420, 430	Medium	6.0
3167430	[CVE-2022-31591] **Privilege Escalation vulnerability in SAP BusinessObjects (BW Publisher Service)** Product - SAP BusinessObjects BW Publisher Service, Versions - 420,430	Medium	5.6
3203079	[CVE-2022-32246] **SQL Injection vulnerability in SAP BusinessObjects Business Intelligence Platform (Visual Difference Application**) Product - SAP BusinessObjects Business Intelligence Platform (Visual Difference Application), Versions - 420, 430	Medium	5.4
3213279	[CVE-2022-31598] **Cross-Site Scripting (XSS) vulnerability in SAP Business Objects** Product - SAP Business Objects, Version - 420	Medium	5.4
3213826	[CVE-2022-31597] **Missing Authorization check in business partner extension for Spain/Slovakia** Product - SAP S/4HANA, Versions - S4CORE 101, 102, 103, 104, 105, 106, SAPSCORE 127	Medium	5.4
3211203	[CVE-2022-35168] **Denial of Service vulnerability in SAP Business One** Product - SAP Business one, Version - 10.0	Medium	4.3
3216161	[CVE-2022-32248] **Missing Input Validation in Manage Checkbooks component of SAP S/4HANA** Product - SAP S/4HANA, Versions - 101, 102, 103, 104, 105, 106	Medium	4.3
3196280	[CVE-2022-31592] **Missing Authorization check in EA-DFPS** Product - SAP Enterprise Extension Defense Forces & Public Security (EA-DFPS), Versions - 605, 606, 616,617,618, 802, 803, 804, 805, 806	Medium	4.3

3220746	[CVE-2022-35171] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** Product - SAP 3D Visual Enterprise Viewer, Version - 9.0	Low	3.3
3155571	***Update to Security Note released on June 2022 Patch Day:*** [CVE-2022-31594] **Privilege escalation vulnerability in SAP Adaptive Server Enterprise (ASE)** Product - SAP Adaptive Server Enterprise (ASE), Versions - KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53	Low	3.2

JUNE 2022

On 14th of June 2022, SAP Security Patch Day saw the release of 10 new Security Notes. Further, there were 2 updates to previously released Patch Day 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, Version - 6.5	Very High	10
3158375	[CVE-2022-27668] **Improper Access Control of SAProuter for SAP NetWeaver and ABAP Platform** Product - SAP NetWeaver and ABAP Platform, Versions - KERNEL 7.49, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.49, KRNL64UC 7.49, SAP_ROUTER 7.53, 7.22	High	8.6
3197005	[CVE-2022-31590] **Potential privilege escalation in SAP PowerDesigner Proxy 16.7** Product - SAP PowerDesigner Proxy 16.7, Versions - 16.7	High	7.8
3165801	***Update to Security Note released on May 2022 Patch Day:*** [CVE-2022-29611] **Missing Authorization check in SAP NetWeaver Application Server for ABAP and ABAP Platform** Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Version - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788	Medium	6.5
3206271	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2022-32235, CVE-2022-32236, CVE-2022-32237, CVE-2022-32238, CVE-2022-32239, CVE-2022-32240, CVE-2022-32241, CVE-2022-32242, CVE-2022-32243 Product - SAP 3D Visual Enterprise Viewer, Version - 9.0	Medium	6.5
3197927	[CVE-2022-29618] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Development Infrastructure (Design Time Repository)** Product - SAP NetWeaver Development Infrastructure (Design Time Repository), Versions - 7.30, 7.31, 7.40, 7.50	Medium	6.1
3194674	[CVE-2022-29612] **Server-Side Request Forgery in SAP NetWeaver, ABAP Platform and SAP Host Agent** Product - SAP NetWeaver, ABAP Platform and SAP Host Agent, Versions - KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, 8.04, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, 8.04, SAPHOSTAGENT 7.22	Medium	5.0
3203065	[CVE-2022-31589] **Segregation of Duty vulnerability in IL FI-AP File from SHAAM program** Product - SAP ERP, localization for CEE countries, Versions - C-CEE 110_600, 110_602, 110_603, 110_604, 110_700 Product - SAP Financials, Versions - SAP_FIN 618, 720 Product - SAP S/4Hana Core, Versions - S4CORE 100, 101, 102, 103, 104, 105, 106, 107, 108	Medium	5.0

3158815	[CVE-2022-31595] **Privilege escalation vulnerability in SAP Financial Consolidation** Product - SAP Adaptive Server Enterprise (ASE), Versions - KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53	Medium	5.0
3158619	[CVE-2022-29614] **Privilege Escalation in SAP startservice of SAP NetWeaver AS ABAP, AS Java, ABAP Platform and HANA Database** Product - SAP NetWeaver AS ABAP, AS Java, ABAP Platform and HANA Database, Versions - KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.88, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, SAPHOSTAGENT 7.2	Medium	4.9
3202846	[CVE-2022-29615] **Multiple vulnerabilities associated with Apache log4j 1.x component in SAP Netweaver Developer Studio (NWDS)** Product - SAP NetWeaver Developer Studio (NWDS), Versions - 7.50	Low	3.4
3155571	[CVE-2022-31594] **Privilege escalation vulnerability in SAP Adaptive Server Enterprise (ASE)** Product - SAP Adaptive Server Enterprise (ASE), Versions - KERNEL 7.22, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53	Low	3.2

MAY 2022

On 10th of May 2022, SAP Security Patch Day saw the release of 8 new Security Notes. Further, there were 4 updates to previously released Patch Day Security Notes.

Note#	Title	Priority	CVSS
3170990	***Update to Security Note released on April 2022 Patch Day:*** [CVE-2022-22965] ***Central Security Note for Remote Code Execution vulnerability associated with Spring Framework***	Hot News	9.8
3189409	[CVE-2022-22965] **Remote Code Execution vulnerability associated with Spring Framework used in SAP Business One Cloud** Product - SAP Business One Cloud, Version - 1.1	Hot News	9.8
3171258	[CVE-2022-22965] **Remote Code Execution vulnerability associated with Spring Framework used in SAP Commerce** Product - SAP Commerce, Versions - 1905, 2005, 2105 & 2011	Hot News	9.8
3189635	[CVE-2022-22965] **Remote Code Execution vulnerability associated with Spring Framework used in SAP Customer Profitability Analytics** Product - SAP Customer Profitability Analytics, Version - 2	Hot News	9.8
3145046	[CVE-2022-27656] **Cross-Site Scripting (XSS) vulnerability in administration UI of SAP Webdispatcher and SAP Netweaver AS for ABAP and Java (ICM)** Product - SAP Webdispatcher, Versions - 7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.83, 7.85 Product - SAP Netweaver AS for ABAP and Java (ICM), Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, 8.04, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 8.04.	High	8.3
2998510	[CVE-2022-28214] **Central Management Server Information Disclosure in Business Intelligence Update** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	High	7.8

3137191	*Update to Security Note released on April 2022 Patch Day:* [CVE-2022-22541] **Information Disclosure vulnerability in SAP BusinessObjects Platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	Medium	6.8
3165801	[CVE-2022-29611] **Missing Authorization check in SAP NetWeaver Application Server for ABAP and ABAP Platform** Product - SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, 788	Medium	6.5
3164677	[CVE-2022-29613] **Information Disclosure vulnerability in SAP Employee Self Service (Fiori My Leave Request)** Product - SAP Employee Self Service (Fiori My Leave Request), Version - 605	Medium	6.5
3146336	[CVE-2022-29610] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Application Server ABAP** Product - SAP NetWeaver Application Server ABAP, Versions - 753, 754, 755, 756	Medium	5.4
3158188	[CVE-2022-28774] **Information Disclosure vulnerability in SAP Host Agent logfile** Product - SAP Host Agent, Version - 7.22	Medium	5.3
3145702	[CVE-2022-29616] **Memory Corruption vulnerability in SAP Host Agent, SAP NetWeaver and ABAP Platform** Product - SAP NetWeaver and ABAP Platform, Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, 7.8	Medium	5.3
3124994	*Update to Security Note released on February 2022 Patch Day:* [CVE-2022-22534] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver** Product - SAP NetWeaver (ABAP and Java application Servers), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756	Medium	4.7
3165333	*Update to Security Note released on April 2022 Patch Day:* [CVE-2022-28215] **URL Redirection vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver ABAP Server and ABAP Platform, Versions - 740, 750, 787	Medium	4.7

APRIL 2022

On 12th of April 2022, SAP Security Patch Day saw the release of 23 new Security Notes. Further, there were 10 updates to previously released Patch Day 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, Version – 6.5	Hot News	10
3123396	*Update to Security Note released on February 2022 Patch Day:* [CVE-2022-22536] **Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher** Product - SAP Web Dispatcher, Versions -7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87Product-SAP Content Server, Version -7.53Product-SAP NetWeaver and ABAP Platform, Versions -KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49	Hot News	10

3022622	***Update to Security Note released on March 2021 Patch Day:*** [CVE-2021-21480] **Code injection vulnerability in SAP Manufacturing Integration and Intelligence** Product - SAP Manufacturing Integration and Intelligence, Versions - 15.1, 15.2, 15.3, 15.4	Hot News	9.9
3170990	[CVE-2022-22965] **Central Security Note for Remote Code Execution vulnerability associated with Spring Framework**	Hot News	9.8
3189428	[CVE-2022-22965] **Remote Code Execution vulnerability associated with Spring Framework used in SAP HANA Extended Application Services** Product - SAP HANA Extended Application Services, Version - 1	Hot News	9.8
3187290	[CVE-2022-22965] **Remote Code Execution vulnerability associated with Spring Framework used in SAP Customer Checkout** Product - SAP Customer Checkout, Version - 2.0 Product - SAP Customer Checkout_SVR, Version - 2.0	Hot News	9.8
3189429	[CVE-2022-22965] **Remote Code Execution vulnerability associated with Spring Framework used in PowerDesigner Web (up to including 16.7 SP05 PL01)** Product - SAP Powerdesigner Web Portal, Version - 16.7	Hot News	9.8
3158613	**Update 1 to Security Note 3022622 -** [CVE-2021-21480] **Code injection vulnerability in SAP Manufacturing Integration and Intelligence** Product - SAP Manufacturing Integration and Intelligence, Versions - 15.1, 15.2, 15.3, 15.4	Hot News	9.1
3080567	***Update to Security Note released on September 2021 Patch Day:*** [CVE-2021-38162] **HTTP Request Smuggling in SAP Web Dispatcher** Product - SAP Web Dispatcher, Version - 7.22, 7.49, 7.53, 7.77, 7.81, 7.83	High	8.9
3130497	[CVE-2022-27671] **CSRF token visible in one of the URL in SAP Business Intelligence Platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	High	8.2
3149805	***Update to Security Note released on March 2022 Patch Day:*** [CVE-2022-26101] **Cross-Site Scripting (XSS) vulnerability in SAP Fiori launchpad** Product - Fiori Launchpad, Versions 754, 755, 756	High	8.2
3123427	***Update to Security Note released on February 2022 Patch Day:*** [CVE-2022-22532] **HTTP Request Smuggling in SAP NetWeaver Application Server Java** Additional CVE - CVE-2022-22533 Product - SAP NetWeaver Application Server Java, Versions -KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53	High	8.1
2998510	[CVE-2022-28214] **Central Management Server Information Disclosure in Business Intelligence Update** Product - SAP BusinessObjects Enterprise (Central Management Server), Versions - 420, 430	High	7.8
3111311	[CVE-2022-28772] **Denial of service (DOS) in SAP Web Dispatcher and SAP Netweaver (Internet Communication Manager)** Product - SAP NetWeaver (Internet Communication Manager), Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86 Product - SAP Web Dispatcher, Versions - 7.53, 7.77, 7.81, 7.85, 7.86	High	7.5
3155609	[CVE-2022-23181] **Privilege escalation vulnerability in Apache Tomcat server component of SAP Commerce** Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011	High	7.0
3137191	[CVE-2022-22541] **Information Disclosure vulnerability in SAP BusinessObjects Platform** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	Medium	6.8

3143437	**[Multiple CVEs] Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2022-27655, CVE-2022-26106, CVE-2022-26107, CVE-2022-26109**,** CVE-2022-27654, CVE-2022-26108 Product - SAP 3D Visual Enterprise Viewer, Version - 9	Medium	6.5
3148094	[CVE-2022-27670] **Denial of service (DOS) in SQL Anywhere** Product - SAP SQL Anywhere Server, Version - 17.0	Medium	6.5
3148377	[CVE-2022-28217] **Missing XML Validation vulnerability in SAP NW EP WPC** Product - SAP NetWeaver (EP Web Page Composer), Versions - 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.5
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 - SAPS/4HANA(Supplier Factsheet and Enterprise Search for Business Partner, Supplier and Customer), Versions -104, 105, 106	Medium	6.5
3163703	**Multiple Vulnerabilities in URI.js bundled with SAPUI5** Related CVEs - CVE-2021-27516, CVE-2020-26291, CVE-2021-3647, CVE-2022-0613 Product - SAPUI5, Versions - 750, 753, 754, 755, 756, 200	Medium	6.1
3163583	[CVE-2022-26105] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Version - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3126557	[CVE-2022-28770] **Cross-Site Scripting (XSS) vulnerability in SAPUI5 (vbm library)** Product - SAPUI5 (vbm library), Versions - 750, 753, 754, 755, 756	Medium	6.1
3055044	[CVE-2022-28213] **Missing XML Validation vulnerability in SAP BusinessObjects Business Intelligence Platform (dswsbobje - SOAP Web services)** Product - SAP BusinessObjects Business Intelligence Platform, Versions - 420, 430	Medium	5.4
3145769	[CVE-2022-27667] **Information Disclosure vulnerability in CMC** Product - SAP BusinessObjects Business Intelligence Platform, Version - 430	Medium	5.3
3152442	[CVE-2022-27669] **Missing Authentication check in XML Data Archiving Service** Product - SAP NetWeaver Application Server for Java, Version - 7.50	Medium	5.3
3111293	[CVE-2022-28773] **Denial of service (DOS) in SAP Web Dispatcher and SAP NetWeaver (Internet Communication Manager)** Product - SAP NetWeaver (Internet Communication Manager), Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86 Product - SAP Web Dispatcher, Versions - 7.53, 7.77, 7.81, 7.85, 7.86	Medium	4.9
3128473	***Update to Security Note released on February 2022 Patch Day:*** [CVE-2022-22545] **Information Disclosure vulnerability in SAP NetWeaver Application Server ABAP and ABAP Platform** Product - SAP NetWeaver Application Server ABAP and ABAP Platform, Versions - 700, 710, 711, 730, 731, 740, 750-756	Medium	4.9
3165333	[CVE-2022-28215] **URL Redirection vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver ABAP Server and ABAP Platform, Versions - 740, 750, 787	Medium	4.7
3165856	This security note was released out-of-band prior SAP Security Patch Day (See table below) [CVE-2022-27658] **Missing authorization check in SAP Innovation Management** Product - SAP Innovation Management, Version - 2	Medium	4.3

3150845	[CVE-2022-28216] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (BI Workspace)** Product - SAP BusinessObjects Business Intelligence Platform (BI Workspace), Version - 420	Medium	4.3
3138299	[CVE-2021-44832] **Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP NetWeaver ABAP Server and ABAP Platform (Adobe LiveCycle Designer 11.0)** Product - SAP NetWeaver (Internet Communication Manager, Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86 Product - SAP Web Dispatcher, Versions - 7.53, 7.77, 7.81, 7.85, 7.86	Medium	4.1
3116223	***Update to Security Note released on February 2022 Patch Day:*** [CVE-2022-22543] **Denial of service (DOS) in SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel)** Product - SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel), Versions -KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49	Low	3.7
3159091	[CVE-2022-27657] **Directory Traversal vulnerability in SAP Focused Run (Simple Diagnostics Agent 1.0)** Product - SAP Focused Run (Simple Diagnostics Agent), Version - 1.0	Low	2.7

MARCH 2022 – OUT-OF-BAND RELEASE

Note#	Title	Priority	CVSS
3165856	***3165856 - [CVE-2022-27658] Missing authorization check in SAP Innovation Management*** Product- SAP Innovation Management, Version 2.0	Medium	4.3

MARCH 2022 : LIST OF SECURITY NOTES RELEASED ON MARCH PATCH DAY :

On 8th of March 2022, SAP Security Patch Day saw the release of 12 new Security Notes. Further, there were 4 updates to previously released Patch Day Security Notes.

Note#	Title	Priority	CVSS
3123396	***Update to Security Note released on February 2022 Patch Day:*** [CVE-2022-22536] **Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher** Product- SAP Web Dispatcher, Versions - 7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87 Product- SAP Content Server, Version - 7.53 Product - SAP NetWeaver and ABAP Platform, Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49	Hot News	10
3131047	***Update to Security Note released on December 2021 Patch Day:*** [CVE-2021-44228] **Central Security Note for Remote Code Execution vulnerability associated with Apache Log4j 2 component**	Hot News	10
3154684	[CVE-2021-44228] **Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Work Manager** Additional CVE - CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 Product - SAP Work Manager, Versions 6.4, 6.5, 6.6 Product - SAP Inventory Manager, Versions 4.3, 4.4	Hot News	10

3145987	[CVE-2022-24396] **Missing Authentication check in SAP Focused Run (Simple Diagnostics Agent 1.0)** Product - Simple Diagnostics Agent	Hot News	9.3
3149805	[CVE-2022-26101] **Cross-Site Scripting (XSS) vulnerability in SAP Fiori launchpad** Product - Fiori Launchpad, Versions 754, 755, 756	High	8.2
1753378	***Update to Security Note released on August 2013 Patch Day:*** **Directory traversal in Web Container** Product - SAP-JEE, Version 6.40 Product - SAP-JEECOR, Versions 6.40, 7.00, 7.01 Product - SERVERCORE, Versions 7.10, 7.11, 7.20, 7.30, 7.31	Medium	5.3
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
3146261	[CVE-2022-24395] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.1
3146260	[CVE-2022-24397] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal, Versions 7.30, 7.31, 7.40, 7.50	Medium	6.1
3144941	[CVE-2022-26104] **Missing Authorization check in SAP Financial Consolidation** Product - SAP Financial Consolidation, Version 10.1	Medium	5.4
3145997	[CVE-2022-26102] **Missing authorization check in SAP NetWeaver Application Server for ABAP** Product - SAP NetWeaver Application Server for ABAP, Versions 700, 701, 702, 731	Medium	5.4
3147283	[CVE-2022-24399] **Cross-Site Scripting (XSS) vulnerability in SAP Focused Run (Real User Monitoring)** Product - SAP Focused Run, Versions 200, 300	Medium	5.4
3147102	[CVE-2022-22547] **Information Disclosure vulnerability in SAP Focused Run (Simple Diagnostics Agent 1.0)** Product - Simple Diagnostics Agent, Versions =>1.0, < 1.58	Medium	5.3
3103424	[CVE-2022-24398] **Information Disclosure vulnerability in SAP Business Objects Business Intelligence Platform** Product - SAP Business Objects Business Intelligence Platform, Version 420, 430	Medium	5.0
3111110	[CVE-2022-26100] **Denial of service (DOS) in SAPCAR** Product - SAPCAR, Version 7.22	Medium	4.8
3132360	[CVE-2022-26103] **Information Disclosure vulnerability in SAP NetWeaver(Real Time Messaging Framework)** Product - SAP NetWeaver AS JAVA (Portal Basis), Version 7.50	Low	3.7

FEBRUARY 2022 : LIST OF SECURITY NOTES RELEASED ON FEBRUARY PATCH DAY :

On 8th of February 2022, SAP Security Patch Day saw the release of 13 new Security Notes. 1 security note was released out-of-band. Further, there were 5 updates to previously released Patch Day Security Notes.

Note#	Title	Priority	CVSS
3123396	[CVE-2022-22536] **Request smuggling and request concatenation in SAP NetWeaver, SAP Content Server and SAP Web Dispatcher** Product - SAP Web Dispatcher, Versions - 7.49, 7.53, 7.77, 7.81, 7.85, 7.22EXT, 7.86, 7.87 Product - SAP Content Server, Version - 7.53 Product - SAP NetWeaver and ABAP Platform, Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49	Hot News	10
3142773	[CVE-2021-44228] **Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Commerce** Related CVEs - CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011	Hot News	10
3130920	**Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Data Intelligence 3 (on-premise)** Related CVEs - CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 Product - SAP Data Intelligence, Version - 3	Hot News	10
3139893	[CVE-2021-44228] **Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Dynamic Authorization Management** Related CVEs - CVE-2021-44228, CVE-2021-45046 Product - SAP Dynamic Authorization Management, Version - 9.1.0.0, 2021.03	Hot News	10
3132922	***Update to Security Note released in December 2021:*** [CVE-2021-44228] **Remote Code Execution vulnerability associated with Apache Log4j 2 component used in Internet of Things Edge Platform** Related CVEs - CVE-2021-45105, CVE-2021-45046 , CVE-2021-44832 Product - Internet of Things Edge Platform, Version - 4.0	Hot News	10
3133772	***Update to Security Note released in December 2021:*** [CVE-2021-44228] **Remote Code Execution vulnerability associated with Apache Log4j 2 component used in SAP Customer Checkout** Related CVEs - CVE-2021-45046, CVE-2021-45105 Product - SAP Customer Checkout, Version - 2	Hot News	10
3131047	***Update to Security Note released in December 2021:*** [CVE-2021-44228] **Central Security Note for Remote Code Execution vulnerability associated with Apache Log4j 2 component**	Hot News	10
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, Version – 6.5	Hot News	10
3140940	[CVE-2022-22544] **Missing segregation of duties in SAP Solution Manager Diagnostics Root Cause Analysis Tools** Product - SAP Solution Manager (Diagnostics Root Cause Analysis Tools), Version - 720	Hot News	9.1
3112928	***Update to Security Note released on January 2022 Patch Day:*** [CVE-2022-22531] **Multiple vulnerabilities in F0743 Create Single Payment application of SAP S/4HANA** Additional CVE - CVE-2022-22530 Product - SAP S/4HANA, Versions - 100, 101, 102, 103, 104, 105, 106	High	8.7
3123427	[CVE-2022-22532] **HTTP Request Smuggling in SAP NetWeaver Application Server Java** Product - SAP NetWeaver Application Server Java, Versions - KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53	High	8.1

3140587	[CVE-2022-22540] **SQL Injection vulnerability in SAP NetWeaver AS ABAP (Workplace Server)** Product - SAP NetWeaver AS ABAP (Workplace Server), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787	High	7.1
3124994	[CVE-2022-22534] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver** Product - SAP NetWeaver (ABAP and Java application Servers), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756	Medium	4.7
3126489	[CVE-2022-22535] **Missing Authorization check in SAP ERP HCM** Product - SAP ERP HCM (Portugal), Versions - 600, 604, 608	Medium	6.5
3126748	[CVE-2022-22546] **XSS vulnerability in SAP Business Objects Web Intelligence (BI Launchpad)** Product - SAP Business Objects Web Intelligence (BI Launchpad), Version - 420	Medium	5.4
3134684	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2022-22537, CVE-2022-22739, CVE-2022-22538 Product - SAP 3D Visual Enterprise Viewer , Version - 9.0	Medium	4.3
3140564	[CVE-2022-22528] **Information Disclosure in SAP Adaptive Server Enterprise** Product - SAP Adaptive Server Enterprise, Version - 16.0	Medium	5.6
3142092	[CVE-2022-22542] I**nformation 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
3116223	[CVE-2022-22543] **Denial of service (DOS) in SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel)** Product - SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel) , Versions - KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49	Low	3.7

www.sap.com/contactsap

THE BEST RUN SAP