SAP Security Patch Day – January 2021

Created by Risham Guram, last modified by Aditi Kulkarni on May 12, 2021

This post by SAP Product Security Response Team 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.*

On 12th of January 2021, SAP Security Patch Day saw the release of 10 Security Notes. There were 7 updates to previously released Patch Day Security Notes.

List of security notes released on January Patch Day:

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
2986980	[CVE-2021-21465] **Multiple vulnerabilities in SAP Business Warehouse (Database Interface)** Additional CVE - CVE-2021-21468 Product - SAP Business Warehouse, Versions - 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 782	Hot News	9.9
2999854	[CVE-2021-21466] **Code Injection in SAP Business Warehouse and SAP BW/4HANA** Product - SAP Business Warehouse, Versions - 700, 701, 702, 711, 730, 731, 740, 750, 782 Product - SAP BW4HANA, Versions - 100, 200	Hot News	9.9
2983367	***Update to security note released on December 2020 Patch Day:*** [CVE-2020-26838] **Code Injection vulnerability in SAP Business Warehouse (Master Data Management) and SAP BW4HANA** Product - SAP Business Warehouse, Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 782 Product - SAP BW4HANA, Versions - 100, 200	Hot News	9.1
2979062	***Update to security note released on November 2020 Patch Day:*** [CVE-2020-26820] **Privilege escalation in SAP**	Hot News	9.1

	NetWeaver Application Server for Java (UDDI Server) Product - SAP NetWeaver AS JAVA, Versions - 7.20, 7.30, 7.31, 7.40, 7.50		
3000306	[CVE-2021-21446] **Denial of service (DOS) in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP, Versions - 740, 750, 751, 752, 753, 754, 755	High	7.5
2863397	***Update to security note released on January 2020 Patch Day:*** [CVE-2020-6307] **Missing Authorization Check in Automated Note Search Tool (SAP_BASIS)** Product - Automated Note Search Tool (SAP Basis), Versions - 7.0, 7.01,7.02, 7.31, 7.4, 7.5, 7.51, 7.52, 7.53 and 7.54	Medium	6.5
2826528	***Update to security note released on April 2020 Patch Day:*** [CVE-2020-6224] **Information Disclosure in SAP NetWeaver Application Server Java (HTTP Service)** Product - SAP NetWeaver AS Java (HTTP Service), Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.2
2984034	[CVE-2021-21445] **Header Manipulation vulnerability in SAP Commerce Cloud** Product - SAP Commerce Cloud, Versions - 1808, 1811, 1905, 2005, 2011	Medium	5.4
2965154	[CVE-2021-21447] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (Web Intelligence HTML interface)** Product - SAP BusinessObjects Business Intelligence platform (Web Intelligence HTML interface), Versions - 410, 420	Medium	5.4
2912747	***Update to security note released on May 2020 Patch Day:*** [CVE-2020-6256] **Missing Authorization check in SAP Master Data Governance** Product - SAP Master Data Governance, Versions - 748, 749, 750, 751, 752, 800, 801, 802, 803, 804	Medium	5.4
2971163	***Update to security note released on December 2020 Patch Day:***	Medium	5.4

	[CVE-2020-26816] **Missing Encryption in SAP NetWeaver AS Java (Key Storage Service)** Product - SAP NetWeaver AS JAVA (Key Storage Service), Versions - 7.10, 7.11, 7.20 ,7.30, 7.31, 7.40, 7.50		
2992269	[CVE-2021-21448] **Information Disclosure in SAP GUI for Windows** Product - SAP GUI FOR WINDOWS, Version - 7.60	Medium	5.3
2993032	[CVE-2021-21469] **Information Disclosure in SAP NetWeaver Master Data Management** Product - SAP NetWeaver Master Data Management, Versions - 7.10, 7.10.750, 710	Medium	5.3
3002617	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2021-21449, CVE-2021-21457, CVE-2021-21458, CVE-2021-21459, CVE-2021-21450, CVE-2021-21451, CVE-2021-21452, CVE-2021-21453, CVE-2021-21454, CVE-2021-21455, CVE-2021-21456, CVE-2021-21460, CVE-2021-21461, CVE-2021-21462, CVE-2021-21463, CVE-2021-21464 Product - SAP 3D Visual Enterprise Viewer, Version - 9.0	Medium	4.3
3008422	[CVE-2021-21467] **Missing Authorization check in SAP Banking Services (Generic Market Data)** Product - SAP Banking Services (Generic Market Data), Versions - 400, 450, 500	Medium	4.3
3000291	[CVE-2021-21470] **XML External Entity vulnerability in SAP EPM add-in** Product - SAP EPM ADD-IN, Versions - 2.8, 1010	Low	3.6

, _____

Vulnerability Type Distribution - January 2021

#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (August 2020 – January 2021)**

** 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 take a look at all Security Notes published or updated after December 08, 2020, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'December 10, 2020 - January 12, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – February 2021

Created by Risham Guram, last modified on Apr 12, 2021

This post by SAP Product Security Response Team 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.*

On 9th of February 2021, SAP Security Patch Day saw the release of 7 Security Notes. There were 6 updates to previously released Patch Day Security Notes.

List of security notes released on February Patch Day:

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
3014121	[CVE-2021-21477] **Remote Code Execution vulnerability in SAP Commerce** Product - SAP Commerce, Versions - 1808,1811,1905,2005,2011	Hot News	9.9
2986980	***Update to security note released on January 2021 Patch Day:*** [CVE-2021-21465] **Multiple vulnerabilities in SAP Business Warehouse (Database Interface)** Additional CVE - CVE-2021-21468 Product - SAP Business Warehouse, Versions - 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 782	Hot News	9.9
2993132	***Update to security note released on December 2020 Patch Day:*** [CVE-2020-26832] **Missing Authorization check in SAP NetWeaver AS ABAP and SAP S4 HANA (SAP Landscape Transformation)** Product - SAP NetWeaver AS ABAP (SAP Landscape Transformation - DMIS), Versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 Product - SAP S4 HANA (SAP Landscape Transformation), Versions - 101, 102, 103, 104, 105	High	7.6

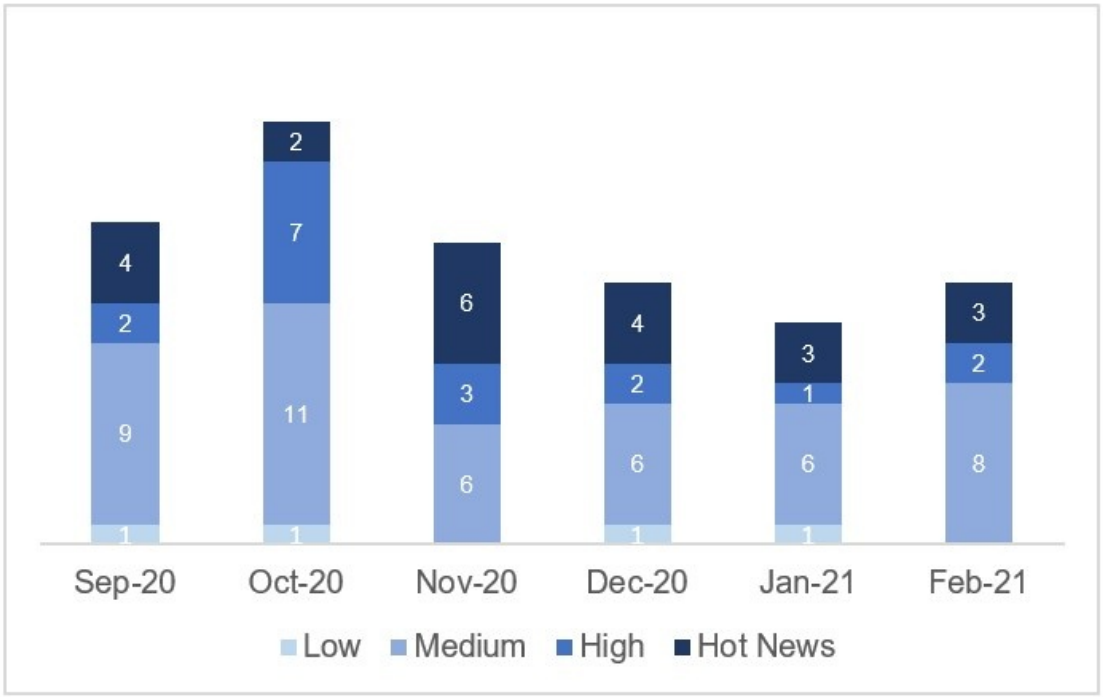
3000306	***Update to security note released on January 2021 Patch Day:*** [CVE-2021-21446] **Denial of service (DOS) in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP, Versions - 740, 750, 751, 752, 753, 754, 755	High	7.5
2998173	[CVE-2021-21472] **Server password not set during installation of SAP NetWeaver Master Data Management 7.1** Product - SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1), Version - 1.0	Medium	6.3
2789866	***Update to security note released on August 2019 Patch Day:*** [CVE-2019-0337] **Cross-Site Scripting (XSS) vulnerability in Java Proxy Runtime of SAP NetWeaver Process Integration** Product - SAP NetWeaver Process Integration (Java Proxy Runtime), Versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50	Medium	6.1
2935791	[CVE-2021-21444] **Clickjacking vulnerability in SAP Business Objects Business Intelligence Platform (CMC and BI Launchpad)** Product - SAP Business Objects Business Intelligence Platform (CMC and BI Launchpad), Versions - 410, 420, 430	Medium	5.4
3014303	[CVE-2021-21476] **Reverse Tabnabbing vulnerability in SAPUI5** Product - SAP UI5, Versions - 1.38.49, 1.52.49, 1.60.34, 1.71.31, 1.78.18, 1.84.5, 1.85.4, 1.86.1,	Medium	4.7
2974582	[CVE-2021-21478] **Reverse Tabnabbing vulnerability within SAP Web Dynpro ABAP Applications** Product - SAP Web Dynpro ABAP	Medium	4.7
2843016	***Update to security note released on November 2019 Patch Day:*** [CVE-2019-0388] **Content spoofing vulnerability in UI5 HTTP Handler** Product - SAP UI, Versions - 7.5, 7.51, 7.52, 7.53, 7.54 Product - SAP UI 700, Versions - 2.0	Medium	4.3
2992154	[CVE-2021-21474] **SAML Assertion Signature MD5 Digest Algorithm Vulnerability in SAP HANA Database**	Medium	4.1

	Product - SAP HANA Database, Versions - 1.0, 2.0		
3000897	[CVE-2021-21475] **Directory Traversal vulnerability in SAP NetWeaver Master Data Management 7.1** Product - SAP NetWeaver Master Data Management Server, Versions - 710, 710.750	Medium	4

Vulnerability Type Distribution - February 2021

#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (September 2020 – February 2021)**



** 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 take a look at all Security Notes published or updated after January 12, 2020, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'January 13, 2021 - February 9, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – March 2021

Created by Risham Guram, last modified on Mar 18, 2021

This post by SAP Product Security Response Team 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.*

On 9th of March 2021, SAP Security Patch Day saw the release of 9 Security Notes. There were 4 updates to previously released Patch Day Security Notes.

Edit: Please note, 1 new Security Note was released on 18 March, 2020. The list below reflects the same.

List of security notes released on March Patch Day:

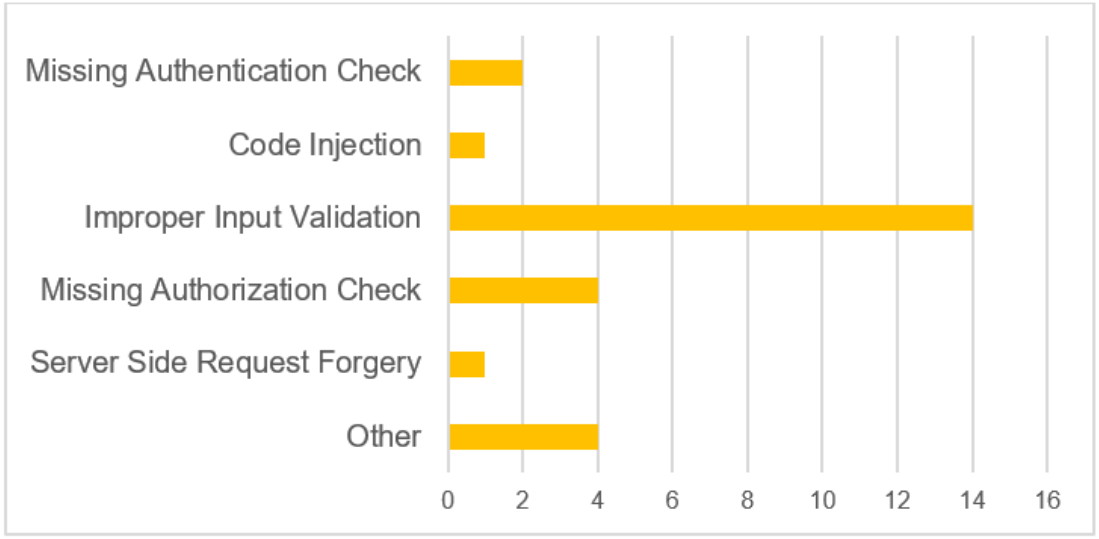
Note#	Title	Priority	CVSS
2890213	***Update to security note released on March 2020 Patch Day:*** [CVE-2020-6207] **Missing Authentication Check in SAP Solution Manager (User-Experience Monitoring)** Product - SAP Solution Manager (User Experience Monitoring), Version - 7.2	Hot News	10
2622660	***Update 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
3022622	[CVE-2021-21480] **Code Injection Vulnerability in SAP MII** Product - SAP Manufacturing Integration and Intelligence, Versions - 15.1, 15.2, 15.3, 15.4	Hot News	9.9
3022422	[CVE-2021-21481] **Missing Authorization Check in SAP NetWeaver AS JAVA (MigrationService)** Product - SAP NetWeaver AS JAVA (MigrationService), Versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50	Hot News	9.6
3017378	[CVE-2021-21484] **Possible authentication bypass in SAP HANA LDAP scenarios** Product - SAP HANA, Version - 2.0	High	7.7
3007888	[CVE-2021-21486] **Missing Authorization check in SAP Enterprise Financial Services(Bank Customer**	Medium	6.8

	Accounts) Product - SAP Enterprise Financial Services (Bank Customer Accounts), Versions - 101, 102, 103, 104, 105, 600, 603, 604, 605, 606, 616, 617, 618, 800		
2983436	[CVE-2021-21488] **Insecure Deserialisation in SAP NetWeaver Knowledge Management** Product - SAP NetWeaver Knowledge Management, Versions - 7.01, 7.02, 7.30,7.31, 7.40, 7.50	Medium	6.8
3023778	[CVE-2021-21487] **Missing Authorization Check in Payment Engine** Product - SAP Payment Engine, Version - 500	Medium	6.8
2943844	***Update to security note released on October 2020 Patch Day:*** [CVE-2020-6308] **Server-Side Request Forgery vulnerability in SAP BusinessObjects Business Intelligence Platform (Web Services)** Product - SAP BusinessObjects Business Intelligence Platform (Web Services), Versions - 410, 420, 430	Medium	5.3
2976947	[CVE-2021-21491] **Reverse TabNabbing vulnerability in SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java)** Product - SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java), Versions - 7.00, 7.10, 7.11, 7.20, 7.30, 731, 7.40, 7.50	Medium	4.7
3027767	[CVE-2021-27592] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** Product - SAP 3D Visual Enterprise Viewer, Version - 9	Medium	4.3
3027758	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** Related CVEs - CVE-2021-27585, CVE-2021-27586, CVE-2021-27587, CVE-2021-21493, CVE-2021-27588, CVE-2021-27591, CVE-2021-27584, CVE-2021-27589, CVE-2021-27590 Product - SAP 3D Visual Enterprise Viewer, Version - 9	Medium	4.3
2944188	***Update to security note released on November 2020 Patch Day:*** [CVE-2020-6316] **Missing Authorization Check in SAP ERP and SAP S/4 HANA** Product - SAP ERP, Versions - 600, 602, 603, 604, 605,	Medium	4.3

	606, 616, 617, 618 Product - SAP S/4 HANA, Versions - 100, 101, 102, 103, 104		
3035472	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** Related CVEs - CVE-2021-27596, CVE-2021-27594, CVE-2021-27593, CVE-2021-27595 Product - SAP 3D Visual Enterprise Viewer, Version - 9	Medium	4.3

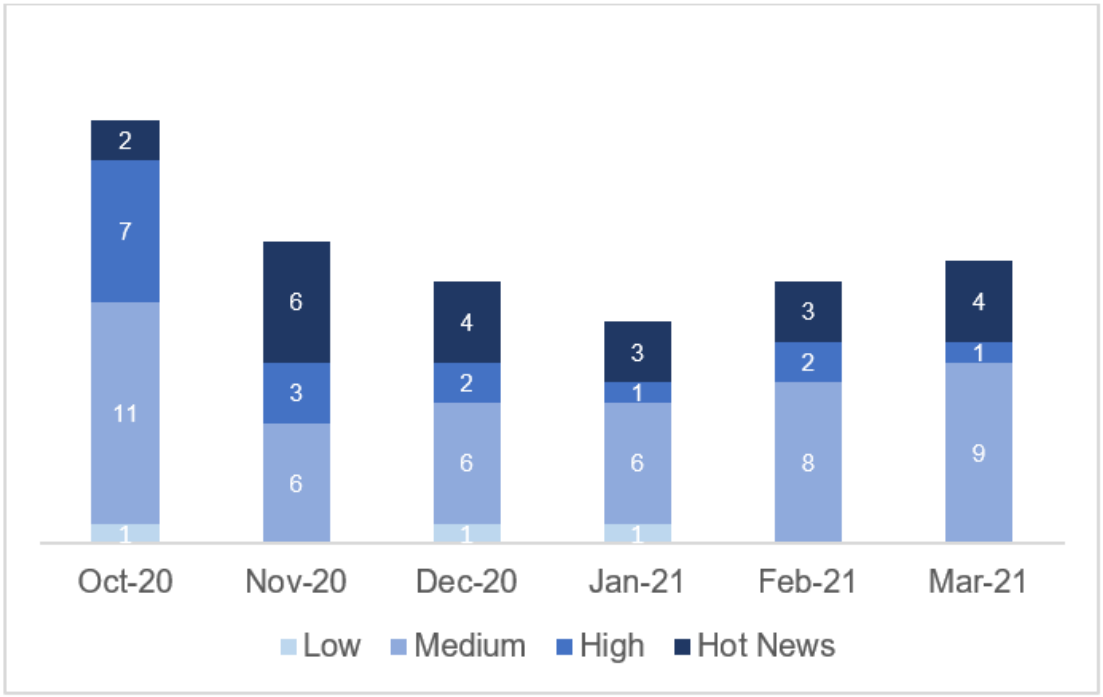
, _____

Vulnerability Type Distribution - March 2021



#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (October 2020 – March 2021)**



** 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 take a look at all Security Notes published or updated after February 9, 2020, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'February 10, 2021 - March 9, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – April 2021

Created by Risham Guram on Apr 13, 2021

This post by SAP Product Security Response Team 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.*

On 13th of April 2021, SAP Security Patch Day saw the release of 14 Security Notes. There were 5 updates to previously released Patch Day Security Notes.

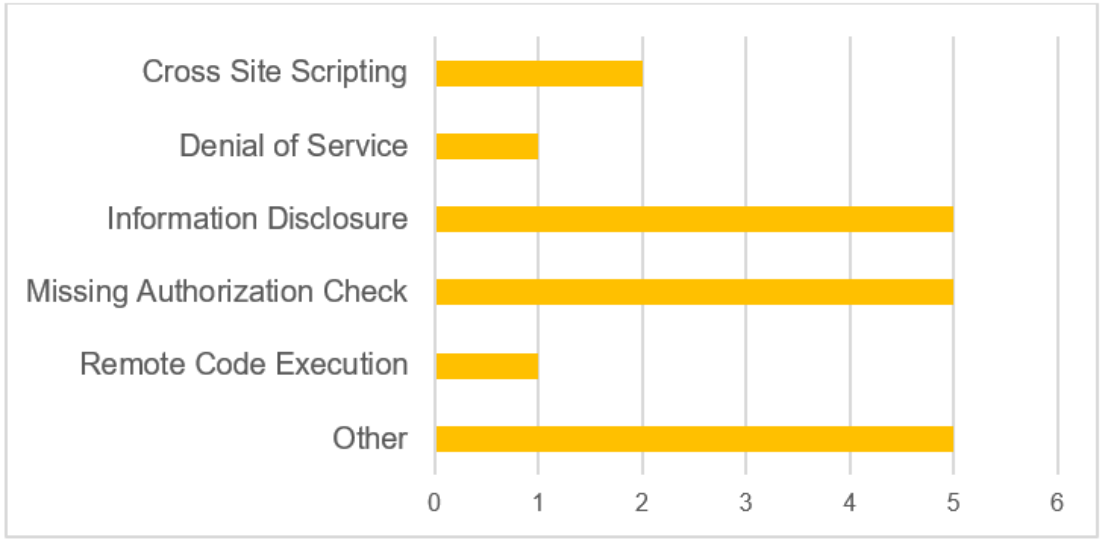
List of security notes released on April Patch Day:

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on August 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
3040210	[CVE-2021-27602] **Remote Code Execution vulnerability in Source Rules of SAP Commerce** Product - SAP Commerce, Versions - 1808, 1811, 1905, 2005, 2011	Hot News	9.9
3022422	***Update to Security Note released on March 2021 Patch Day:*** [CVE-2021-21481] **Missing Authorization Check in SAP NetWeaver AS JAVA (MigrationService)** Product - SAP NetWeaver AS JAVA (MigrationService), Versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50	Hot News	9.6
3017908	[CVE-2021-21482] **Information Disclosure in SAP NetWeaver Master Data Management** Product - SAP NetWeaver Master Data Management, Versions - 710, 710.750	High	8.3
3017823	[CVE-2021-21483] **Information Disclosure in SAP Solution Manager** Product - SAP Solution Manager, Version - 7.20	High	8.2
2993132	***Update to Security Note released on December 2020 Patch Day:*** [CVE-2020-26832] **Missing Authorization check in SAP NetWeaver AS ABAP and SAP S4 HANA (SAP Landscape Transformation)**	High	7.6

	Product - SAP NetWeaver AS ABAP (SAP Landscape Transformation - DMIS), Versions - 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 2011_1_731, 2011_1_752, 2020 Product - SAP S4 HANA (SAP Landscape Transformation), Versions - 101, 102, 103, 104, 105		
3039649	[CVE-2021-27608] **Unquoted Search Path in SAPSetup** Product - SAP Setup, Version - 9.0	High	7.5
3001824	[CVE-2021-21485] **Information Disclosure in SAP NetWeaver AS for Java (Telnet Commands)** Product - SAP NetWeaver AS for JAVA (Telnet Commands), Versions - ENGINEAPI - 7.30, 7.31, 7.40, 7.50, ESP_FRAMEWORK - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, SERVERCORE - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, J2EE-FRMW - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50	High	7.4
3027937	[CVE-2021-27598] **Improper Access Control in SAP NetWeaver AS for Java (Customer Usage Provisioning Servlet)** Product - SAP NetWeaver AS for JAVA (Customer Usage Provisioning Servlet), Versions - 7.31, 7.40, 7.50	Medium	6.5
3028729	[CVE-2021-27603] **Denial of Service(DoS) in SAP NetWeaver AS of ABAP** Product - SAP NetWeaver AS for ABAP, Versions - 731, 740, 750	Medium	6.5
3012277	[CVE-2021-27599] **Information Disclosure in SAP Process Integration (Integration Builder Framework)** Product - SAP Process Integration (Integration Builder Framework), Versions - 7.10, 7.30, 7.31, 7.40, 7.50	Medium	6.5
3036436	[CVE-2021-27604] **Potential XXE Vulnerability in SAP Process Integration (ESR Java Mappings)** Product - SAP Process Integration (Enterprise Service Repository JAVA Mappings), Versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	6.5
3024414	[CVE-2021-27600] **Cross-Site Scripting (XSS) vulnerability in SAP Manufacturing Execution (System Rules)** Product - SAP Manufacturing Execution (System Rules), Versions - 15.1, 15.2, 15.3, 15.4	Medium	6.4
2963592	[CVE-2021-27601] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS Java (Applications based on HTMLB for**	Medium	5.4

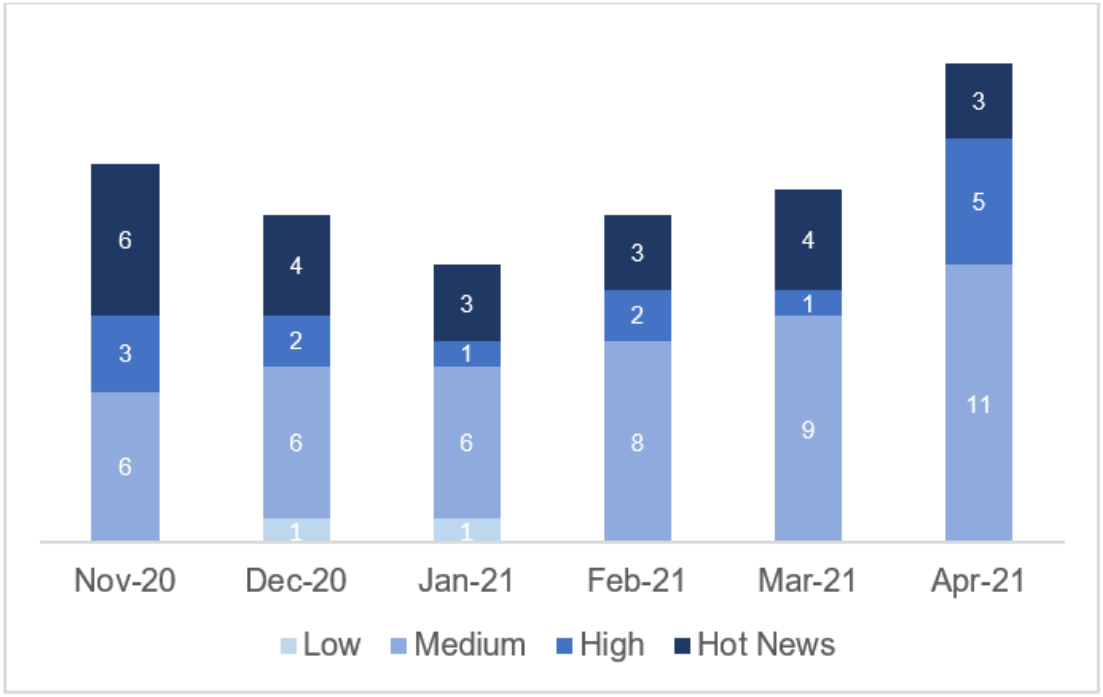
	Java) Product - SAP NetWeaver AS for Java (Applications based on HTMLB for Java) , Versions - EP-BASIS - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50, FRAMEWORK-EXT - 7.30, 7.31, 7.40, 7.50, FRAMEWORK - 7.10, 7.11		
3036679	***Update to Security Note released on October 2011 Patch Day:*** **Update 1 to Security Note 1576763: Potential information disclosure relating to usernames** Product - SAP NetWeaver AS ABAP , Versions - 7.30	Medium	5.3
2976947	***Update to Security Note released on March 2021 Patch Day:*** [CVE-2021-21491] **Reverse TabNabbing vulnerability in SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java)** Product - SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java), Versions - 7.00, 7.10, 7.11, 7.20, 7.30, 731, 7.40, 7.50	Medium	4.7
3030948	[CVE-2021-27609] **Missing Authorization check in SAP Focused RUN** Product - SAP Focused RUN, Versions - 200, 300	Medium	4.6
3025637	[CVE-2021-21492] **Content spoofing in NetWeaver AS Java HTTP Service** Product - SAP NetWeaver AS for JAVA (HTTP Service), Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	4.3
3025054	[CVE-2021-27605] **Missing Authorization check in HCM Travel Management Fiori Apps V2** Product - SAP Fiori Apps 2.0 for Travel Management in SAP ERP, Version - 608	Medium	4.3

Vulnerability Type Distribution - April 2021



#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (November 2020 – April 2021)**



** 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 take a look at all Security Notes published or updated after March 9, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'March 10, 2021 - April 13, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – May 2021

Created by Risham Guram, last modified by Aditi Kulkarni on May 17, 2021

This post by SAP Product Security Response Team 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.*

On 11th of May 2021, SAP Security Patch Day saw the release of 6 Security Notes. There were 5 updates to previously released Patch Day Security Notes.

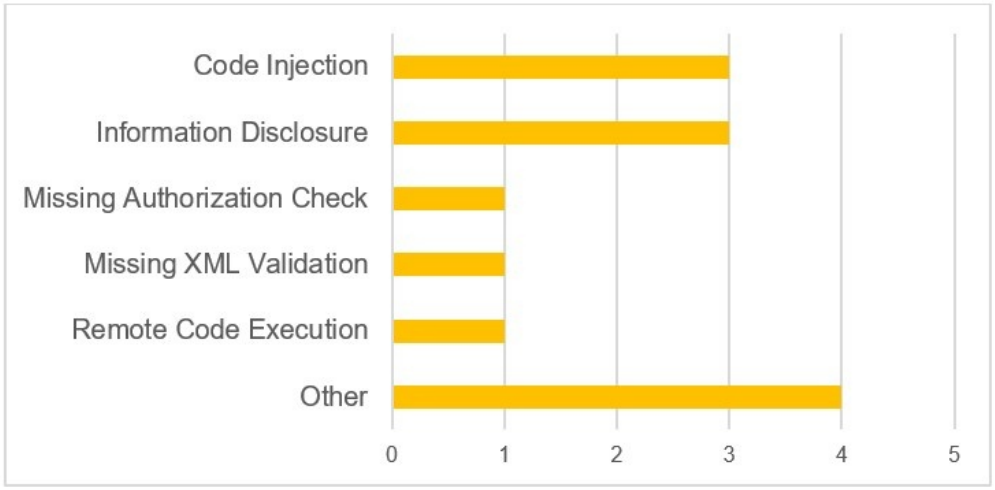
List of security notes released on May Patch Day:

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on August 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
3040210	***Update to Security Note released on April 2021 Patch Day:*** [CVE-2021-27602] **Remote Code Execution vulnerability in Source Rules of SAP Commerce** Product - SAP Commerce, Versions - 1808, 1811, 1905, 2005, 2011	Hot News	9.9
2999854	***Update to Security Note released on January 2021 Patch Day:*** [CVE-2021-21466] **Code Injection in SAP Business Warehouse and SAP BW/4HANA** Product - SAP Business Warehouse, Versions - 700, 701, 702, 711, 730, 731, 740, 750, 782 Product - SAP BW4HANA, Versions - 100, 200	Hot News	9.9
3046610	[CVE-2021-27611] **Code Injection vulnerability in SAP NetWeaver AS ABAP** Product - SAP NetWeaver AS ABAP, Versions - 700,701,702,730,731	High	8.2
3049661	[CVE-2021-27616] **Multiple vulnerabilities in SAP Business One, version for SAP HANA (Business-One-Hana-Chef-Cookbook)** Additional CVE - CVE-2021-27614	High	7.8

	Product - SAP Business One, version for SAP HANA (Cookbooks), Versions - 0.1.6, 0.1.7, 0.1.19		
3049755	[CVE-2021-27613] **Information Disclosure in SAP Business One (Chef business-one-cookbook)** Product - SAP Business One (Cookbooks), Version - 0.1.9	High	7.8
3039818	[CVE-2021-27619] **Information Disclosure in SAP Commerce (Backoffice search)** Product - SAP Commerce (Backoffice Search), Versions - 1808, 1811, 1905, 2005, 2011	Medium	6.5
3012021	[Multiple CVEs] **Multiple vulnerabilities in SAP Process Integration (Integration Builder Framework)** CVEs - CVE-2021-27617, CVE-2021-27618 Product - SAP Process Integration (Integration Builder Framework), Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	4.9
2976947	***Update to Security Note released on March 2021 Patch Day:*** [CVE-2021-21491] **Reverse TabNabbing vulnerability in SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java)** Product - SAP NetWeaver Application Server Java (Applications based on Web Dynpro Java), Versions - 7.00, 7.10, 7.11, 7.20, 7.30, 731, 7.40, 7.50	Medium	4.7
3030948	***Update to Security Note released on April 2021 Patch Day:*** [CVE-2021-27609] **Missing Authorization check in SAP Focused RUN** Product - SAP Focused RUN, Versions - 200, 300	Medium	4.6
3023078	[CVE-2021-27612] **SAP GUI for Windows is vulnerable to redirect users to an untrusted website** Product - SAP GUI for Windows, Versions - 7.60, 7.70	Low	3.4

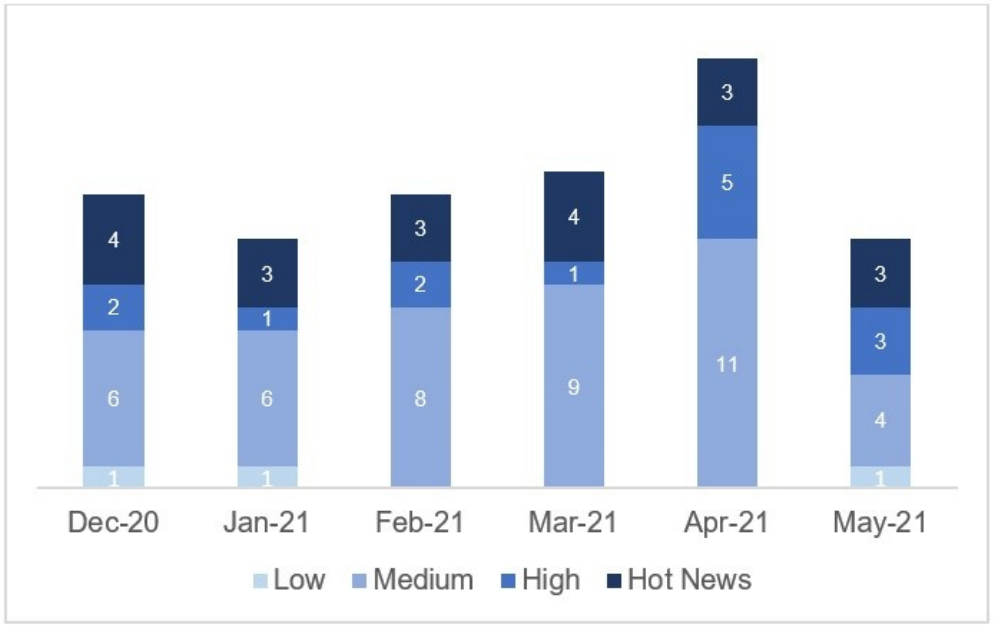
, _____

Vulnerability Type Distribution - May 2021



#Multiple vulnerabilities on same product can be fixed by one security note.

Security Notes vs Priority Distribution (December 2020 – May 2021)**



** 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 take a look at all Security Notes published or updated after April 13, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'April 14, 2021 - May 11, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – June 2021

Created by Risham Guram on Jun 08, 2021

This post by SAP Product Security Response Team 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.*

On 8th of June 2021, SAP Security Patch Day saw the release of 17 Security Notes. There were 2 updates to previously released Patch Day Security Notes.

List of security notes released on June Patch Day:

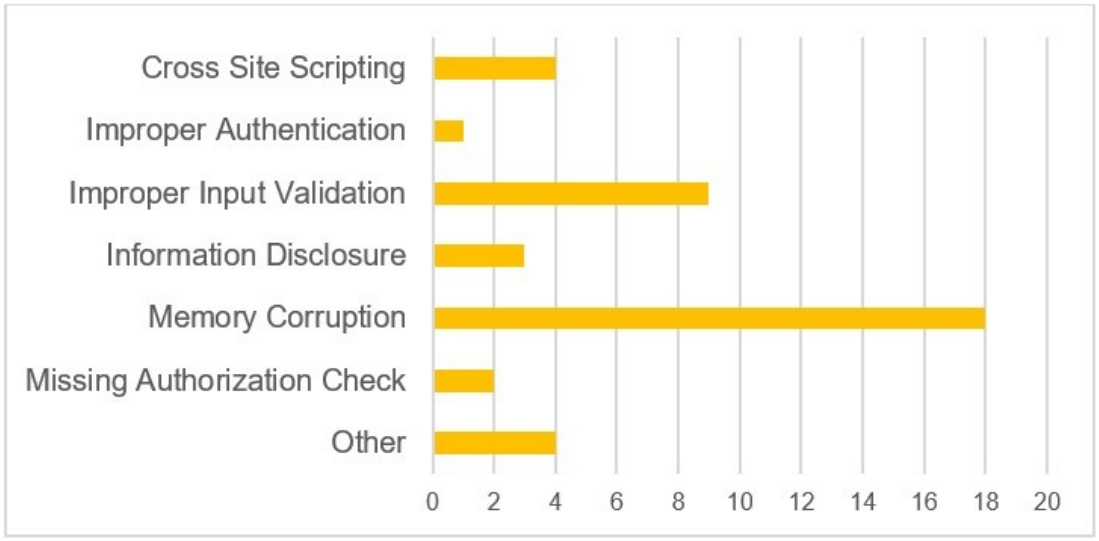
Note#	Title	Priority	CVSS
3040210	***Update to Security Note Released on April 2021 Patch Day:*** [CVE-2021-27602] **Remote Code Execution vulnerability in Source Rules of SAP Commerce** Product- SAP Commerce, Versions - 1808, 1811, 1905, 2005, 2011	Hot News	9.9
3007182	[CVE-2021-27610] **Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700,701,702,731,740,750,751,752,753,754,755,804	Hot News	9
3053066	[CVE-2021-27635] **Missing XML Validation in SAP NetWeaver AS for JAVA** Product - SAP NetWeaver AS for JAVA, Versions - 7.20, 7.30, 7.31, 7.40, 7.50	High	8.7
3020209	[Multiple CVEs] **Memory Corruption vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** CVEs - CVE-2021-27606, CVE-2021-27629, CVE-2021-27630, CVE-2021-27631, CVE-2021-27632 Product - SAP NetWeaver AS for ABAP (RFC Gateway), Versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83	High	7.5
3020104	[Multiple CVEs] **Memory Corruption vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** CVEs - CVE-2021-27597, CVE-2021-27633, CVE-2021-27634 Product - SAP NetWeaver ABAP Server and ABAP Platform	High	7.5

	(Enqueue Server), Versions - KRNL32NUC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73		
3021197	[Multiple CVEs] **Memory Corruption vulnerability in SAP NetWeaver ABAP Server and ABAP Platform** CVEs - CVE-2021-27607, CVE-2021-27628 Product - SAP NetWeaver ABAP Server and ABAP Platform (Dispatcher), Versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83	High	7.5
3058382	[CVE-2021-33662] **Information Disclosure in SAP Business One** Product - SAP Business One, Version - 10.0	Medium	6.7
3030961	[CVE-2021-27615] **Cross-Site Scripting (XSS) vulnerability in SAP Manufacturing Executio**n Product - SAP Manufacturing Execution, Versions - 15.1, 1.5.2, 15.3, 15.4	Medium	6.4
3002517	[CVE-2021-21473] **Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform (SRM_RFC_SUBMIT_REPORT), Versions - 700, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755	Medium	6.3
3004043	[CVE-2021-21490] **Cross-Site Scripting (XSS) vulnerability in SAP Netweaver AS for ABAP (Web Survey)** Product - SAP NetWeaver AS for ABAP (Web Survey), Versions - 700, 702, 710, 711, 730, 731, 750, 750, 752, 75A, 75F	Medium	6.1
3021050	[Multiple CVEs] **Memory Corruption vulnerability in SAP IGS** CVEs - CVE-2021-27620, CVE-2021-27622, CVE-2021-27623, CVE-2021-27624, CVE-2021-27625, CVE-2021-27626, CVE-2021-27627 Product - SAP NetWeaver AS (Internet Graphics Server – Portwatcher), Versions - 7.20,7.20EXT,7.53,7.20_EX2,7.81	Medium	5.9
3049879	[CVE-2021-27637] **Information Disclosure in SAP Enable Now (SAP Workforce Performance Builder - Manager)** Product - SAP Enable Now (SAP Workforce Performance Builder - Manager), Versions - 10.0, 1.0	Medium	5.9

3030604	[CVE-2021-33663] **Plaintext command injection in SAP NetWeaver AS ABAP** Product - SAP NetWeaver AS ABAP, Versions - KRNL32NUC - 7.22,7.22EXT, KRNL32UC - 7.22,7.22EXT, KRNL64NUC - 7.22,7.22EXT,7.49, KRNL64UC - 8.04,7.22,7.22EXT,7.49,7.53,7.73, KERNEL - 7.22,8.04,7.49,7.53,7.73,7.77,7.81,7.82,7.83,7.84	Medium	5.8
3023299	[CVE-2021-27621] **Information Disclosure in SAP NetWeaver AS JAVA (UserAdmin Application)** Product - SAP NetWeaver AS for Java (UserAdmin), Versions - 7.11,7.20,7.30,7.31,7.40,7.50	Medium	5.5
3025604	[CVE-2021-33664] **Cross-Site Scripting (XSS) vulnerability within SAP NetWeaver AS ABAP (Applications based on Web Dynpro ABAP)** Product - SAP NetWeaver Application Server ABAP (Applications based on Web Dynpro ABAP), Versions - SAP_UI – 750,752,753,754,755, SAP_BASIS – 702, 31	Medium	5.4
3028370	[CVE-2021-33665] **Cross-Site Scripting (XSS) vulnerability within SAP NetWeaver AS ABAP (Applications based on SAP GUI for HTML)** Product - SAP NetWeaver Application Server ABAP (Applications based on SAP GUI for HTML), Versions - KRNL64NUC - 7.49, KRNL64UC - 7.49,7.53, KERNEL - 7.49,7.53,7.77,7.81,7.84	Medium	5.4
2985562	[CVE-2021-33666] **MIME Sniffing Vulnerability in SAP Commerce Cloud** Product - SAP Commerce Cloud, Version - 100	Medium	4.7
3059999	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2021-27638, CVE-2021-27639, CVE-2021-27640, CVE-2021-33659, CVE-2021-27642, CVE-2021-33661, CVE-2021-27641, CVE-2021-27643, CVE-2021-33660 Product - SAP 3D Visual Enterprise Viewer, Version - 9	Medium	4.3
3025054	***Update to Security Note Released on April 2021 Patch Day:*** [CVE-2021-27605] **Missing Authorization check in HCM Travel Management Fiori Apps V2** Product - SAP Fiori Apps 2.0 for Travel Management in SAP ERP, Version - 608	Medium	4.3

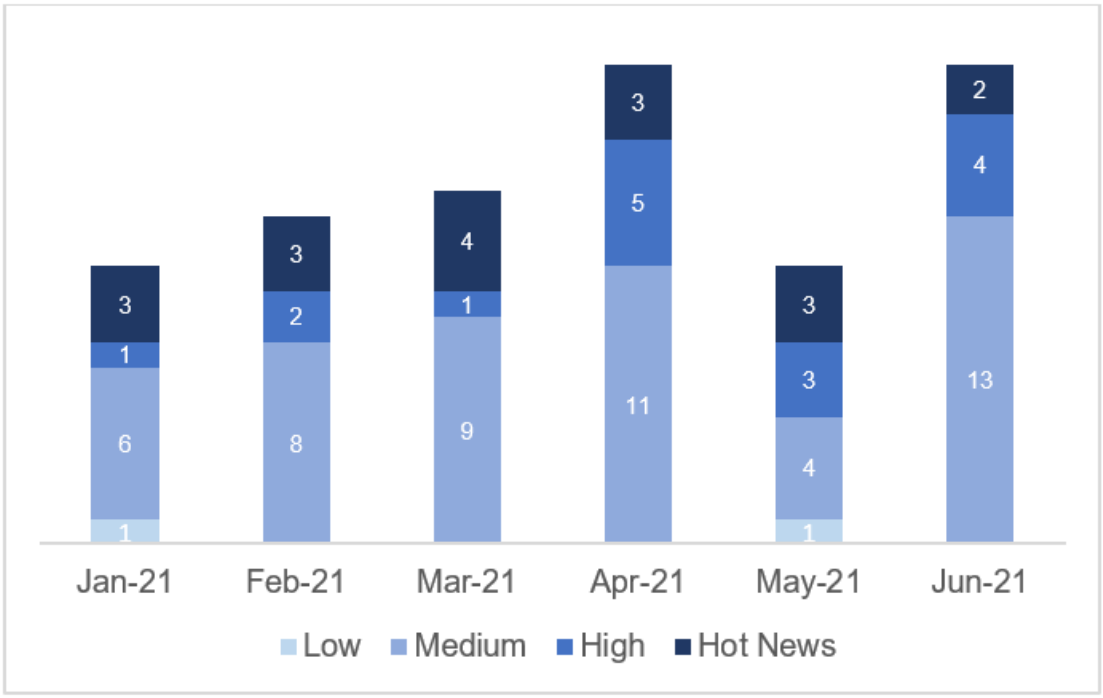
’ _____

Vulnerability Type Distribution - June 2021



#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (January – June 2021)**



** 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 take a look at all Security Notes published or updated after May 11, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'May 12, 2021 - June 8, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – July 2021

Created by Risham Guram, last modified by Aditi Kulkarni on Jul 13, 2021

This post by SAP Product Security Response Team 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.*

On 13th of July 2021, SAP Security Patch Day saw the release of 12 Security Notes. There were 3 updates to previously released Patch Day Security Notes.

List of security notes released on July Patch Day:

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on August 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
3007182	***Update to Security Note released on June 2021 Patch Day:*** [CVE-2021-27610] **Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700,701,702,731,740,750,751,752,753,754,755,804	Hot News	9
3059446	[CVE-2021-33671] **Missing Authorization check in SAP NetWeaver Guided Procedures** Product - SAP NetWeaver Guided Procedures (Administration Workset), Versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50	High	7.6
3056652	[CVE-2021-33670] **Denial of Service (DoS) in SAP NetWeaver AS for Java (Http Service)** Product - SAP NetWeaver AS for Java (Http Service), Versions - 7.10, 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	High	7.5
3066316	[CVE-2021-33676] **Missing authorization check in SAP CRM ABAP** Product - SAP CRM, Versions - 700, 701, 702, 712, 713, 714	Medium	6.8
3036436	***Update to Security Note released on April 2021 Patch***	Medium	6.5

	Day: [CVE-2021-27604] **Potential XXE Vulnerability in SAP Process Integration (ESR Java Mappings)** Product - SAP Process Integration (Enterprise Service Repository JAVA Mappings), Versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50		
3044754	[CVE-2021-33677] **Information Disclosure in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 702, 730, 731, 804, 740, 750, 784, DEV	Medium	6.5
3048657	[CVE-2021-33678] **Code Injection vulnerability in SAP NetWeaver AS ABAP (Reconciliation Framework)** Product - SAP NetWeaver AS ABAP (Reconciliation Framework), Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 75A, 75B, 75B, 75C, 75D, 75E, 75F	Medium	6.5
3053403	[CVE-2021-33682] **Cross-Site Scripting (XSS) vulnerability in SAP Lumira Server** Product - SAP Lumira Server, Version - 2.4	Medium	5.4
3000663	[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
3032624	[CVE-2021-33684] **Memory Corruption in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, 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 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 8.04, 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.53, 7.77, 7.81, 7.84	Medium	5.3
3059764	[CVE-2021-33687] **Information Disclosure in SAP NetWeaver AS for Java (Enterprise Portal)** Product - SAP NetWeaver AS JAVA (Enterprise Portal), Versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50	Medium	4.5

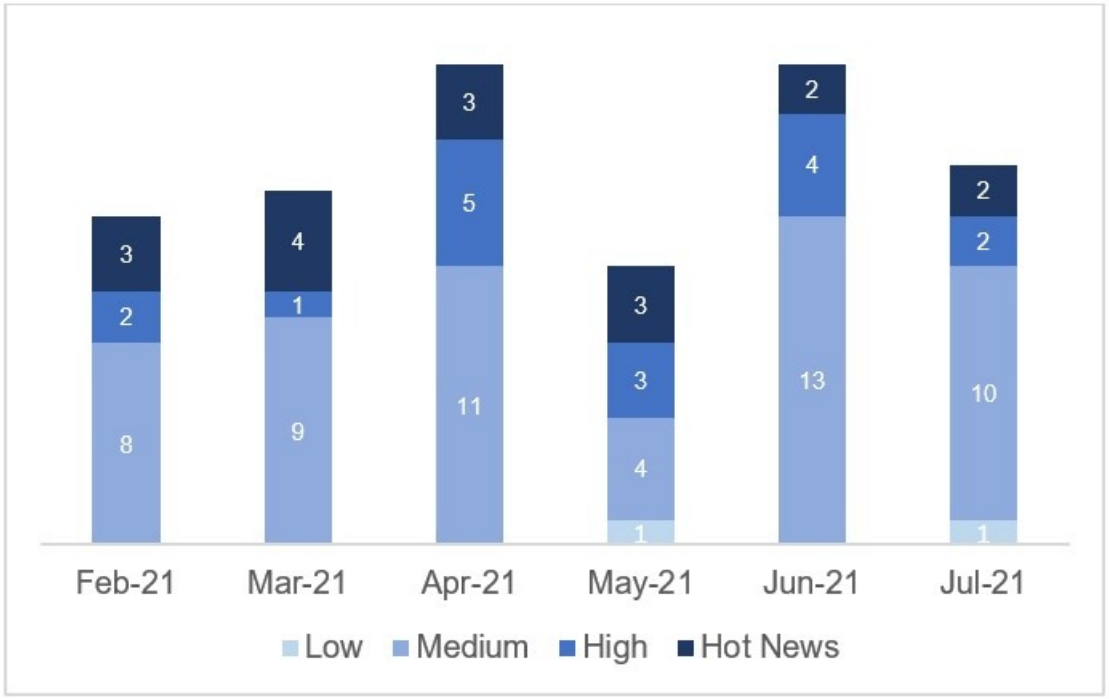
3044751	[CVE-2021-33667] **Information Disclosure in SAP Business Objects Web Intelligence (BI Launchpad)** Product - SAP Business Objects Web Intelligence (BI Launchpad), Versions - 420, 430	Medium	4.3
3067890	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2021-33681, CVE-2021-33680 Product - SAP 3D Visual Enterprise Viewer, Version - 9.0	Medium	4.3
3038594	[CVE-2021-33689] **Insufficient Logging in SAP NetWeaver AS for JAVA (Administrator)** Product - SAP NetWeaver AS JAVA (Administrator applications), Version - 7.50	Low	3.5

, ———

Vulnerability Type Distribution - July 2021

#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (February – July 2021)**



** 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 take a look at all Security Notes published or updated after June 8, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'June 9, 2021 - July 13, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – August 2021

Created by Risham Guram, last modified by Aditi Kulkarni on Aug 10, 2021

This post by SAP Product Security Response Team 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.*

On 10th of August 2021, SAP Security Patch Day saw the release of 14 Security Notes. There were 1 update to previously released Patch Day Security Note.

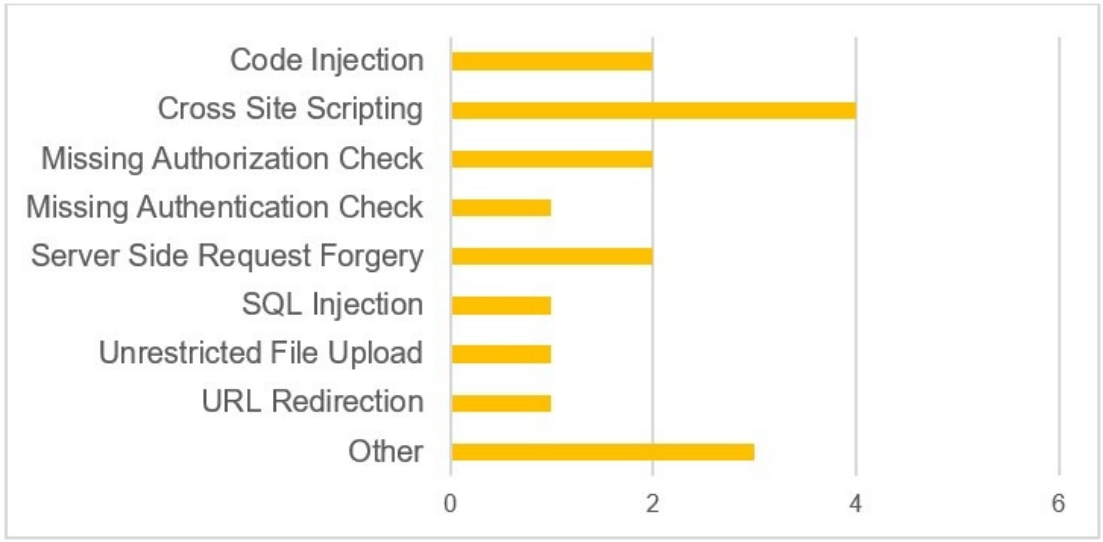
List of security notes released on August Patch Day:

Note#	Title	Severity	CVSS
3071984	[CVE-2021-33698] **Unrestricted File Upload vulnerability in SAP Business One** Product - SAP Business One, Version - 10.0	Hot News	9.9
3072955	[CVE-2021-33690] **Server Side Request Forgery vulnerability in SAP NetWeaver Development Infrastructure (Component Build Service)** Product - SAP NetWeaver Development Infrastructure (Component Build Service), Versions - 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	Hot News	9.9
3078312	[CVE-2021-33701] **SQL Injection vulnerability in SAP NZDT Row Count Reconciliation** Product - DMIS Mobile Plug-In, Versions - DMIS 2011_1_620, 2011_1_640, 2011_1_700, 2011_1_710, 2011_1_730, 710, 2011_1_731, 710, 2011_1_752, 2020 Product - SAP S/4HANA, Versions - SAPSCORE 125, S4CORE 102, 102, 103, 104, 105	Hot News	9.1
3073681	[CVE-2021-33702] **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	High	8.3
3072920	[CVE-2021-33703] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Enterprise Portal** Product - SAP NetWeaver Enterprise Portal	High	8.3

	(Application Extensions), Versions - 7.30, 7.31, 7.40, 7.50		
3074844	[CVE-2021-33705] **Server-Side Request Forgery (SSRF) 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	High	8.1
3067219	[CVE-2021-33699] **Task Hijacking in SAP Fiori Client Native Mobile for Android** Product - SAP Fiori Client Native Mobile for Android, Version - 3.2	High	7.6
3073325	[CVE-2021-33700] **Missing Authentication check in SAP Business One** Product - SAP Business One, Version - 10.0	High	7
3073450	[CVE-2021-33691] **Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Development Infrastructure (Notification Service)** Product - SAP NetWeaver Development Infrastructure (Notification Service), Versions - 7.31, 7.40, 7.50	Medium	6.9
3058553	[CVE-2021-33695] **Multiple Vulnerabilities in SAP Cloud Connector** Additional CVEs - CVE-2021-33694, CVE-2021-33693, CVE-2021-33692 Product - SAP Cloud Connector, Version - 2.0	Medium	6.8
3078072	[CVE-2021-33704] **Missing Authorization Check in SAP Business One (Service Layer)** Product - SAP Business One, Version - 10.0	Medium	6.3
3002517	***Update to Security Note release on June 2021 Patch Day:*** [CVE-2021-21473] **Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform (SRM_RFC_SUBMIT_REPORT), Versions - 700, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755	Medium	6.3
3076399	[CVE-2021-33707] **URL Redirection**	Medium	6.1

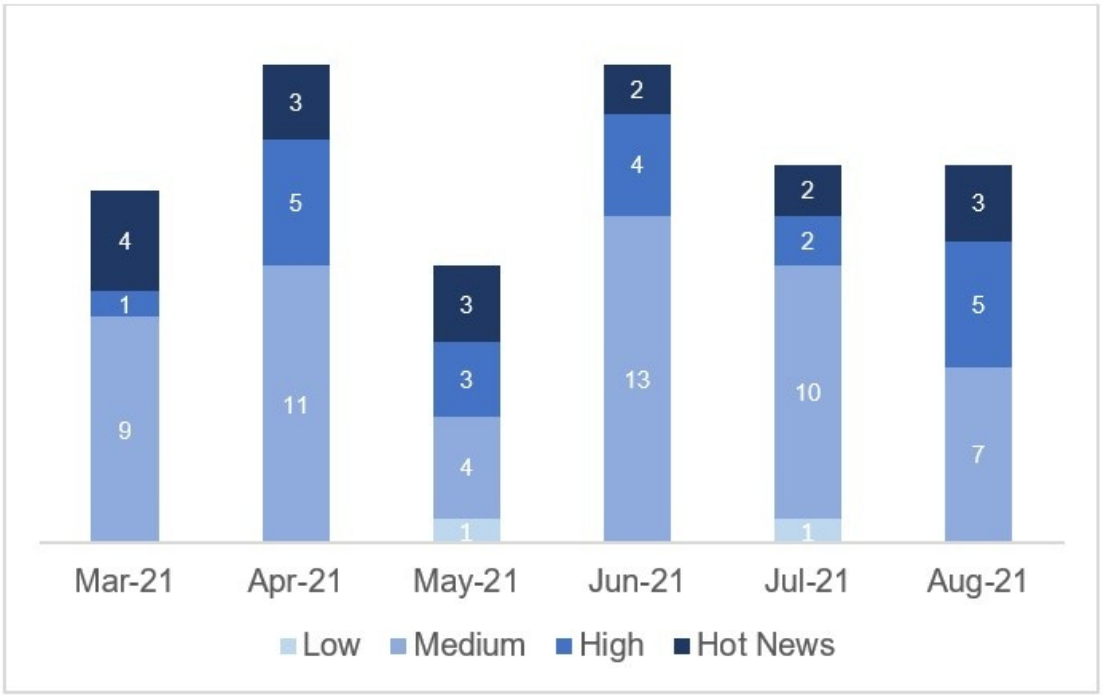
	vulnerability in SAP NetWeaver (Knowledge Management) Product - SAP NetWeaver (Knowledge Management), Versions - 7.30, 7.31, 7.40, 7.50		
3062085	[CVE-2021-33696] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (Crystal Report)** Product - SAP BusinessObjects Business Intelligence Platform (Crystal Report), Versions - 420, 430	Medium	5.4
3063048	[CVE-2021-33697] **Reverse Tabnabbing in SAP BusinessObjects Business Intelligence Platform (SAP UI5)** Product - SAP BusinessObjects Business Intelligence Platform (SAPUI5), Versions - 420, 430	Medium	4.7

Vulnerability Type Distribution - August 2021



#Multiple vulnerabilities on same product can be fixed by one security note.

Security Notes vs Priority Distribution (March – August 2021)**



** 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 take a look at all Security Notes published or updated after July 13, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'July 14, 2021 - August 10, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – September 2021

Created by Risham Guram, last modified by Aditi Kulkarni on Sep 14, 2021

This post by SAP Product Security Response Team 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.*

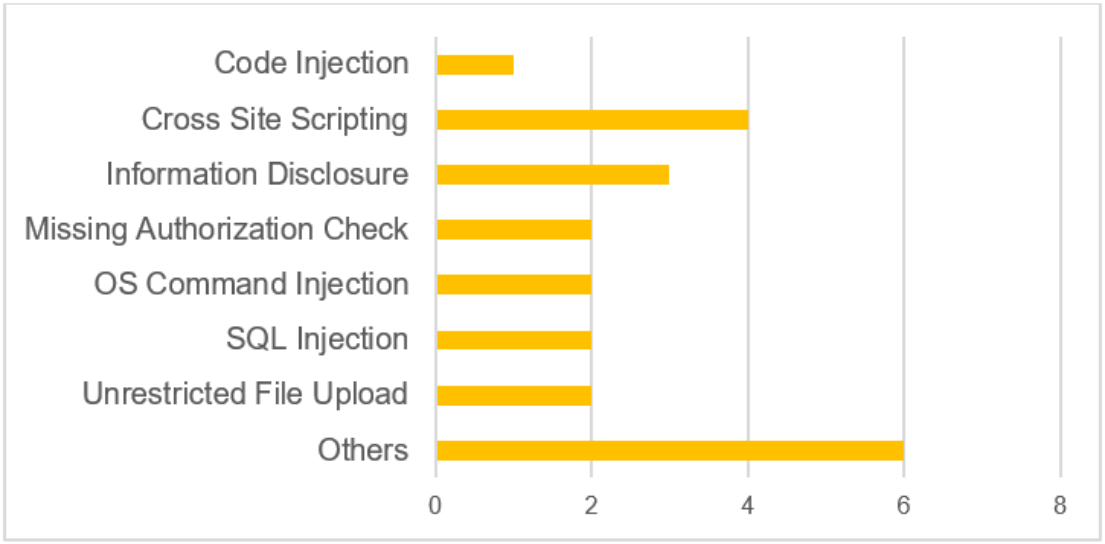
On 14th of September 2021, SAP Security Patch Day saw the release of 17 Security Notes. There were 2 updates to previously released Patch Day Security Note.

List of security notes released on September Patch Day:

Note#	Title	Severity	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	HotNews	10
3078609	[CVE-2021-37535] **Missing Authorization check in SAP NetWeaver Application Server for Java (JMS Connector Service)** Product - SAP NetWeaver Application Server Java (JMS Connector Service) , Versions - 7.11, 7.20, 7.30, 7.31, 7.40, 7.50	HotNews	10
3071984	***Update to Security Note released on August 2021 Patch Day:*** [CVE-2021-33698] **Unrestricted File Upload vulnerability in SAP Business One** Product - SAP Business One, Versions - 10.0	HotNews	9.9
3089831	[CVE-2021-38176] **SQL Injection vulnerability in SAP NZDT Mapping Table Framework** Product - SAP S/4HANA, Versions - 1511, 1610, 1709, 1809, 1909, 2020, 2021 Product - SAP LT Replication Server, Versions - 2.0, 3.0 Product - SAP LTRS for S/4HANA, Version - 1.0 Product - SAP Test Data Migration Server, Version - 4.0 Product - SAP Landscape Transformation, Version - 2.0	HotNews	9.9
3084487	[CVE-2021-38163] **Unrestricted File Upload vulnerability in SAP NetWeaver (Visual Composer 7.0 RT)** Product - SAP NetWeaver (Visual Composer 7.0 RT) , Versions - 7.30, 7.31, 7.40, 7.50	HotNews	9.9
3081888	[CVE-2021-37531] **Code Injection vulnerability in SAP NetWeaver Knowledge Management (XMLForms)** Product - SAP NetWeaver Knowledge Management XML Forms , Versions - 7.10, 7.11, 7.30, 7.31, 7.40, 7.50	HotNews	9.9
3073891	[CVE-2021-33672] **Multiple vulnerabilities in SAP Contact Center** Additional CVEs - CVE-2021-33673, CVE-2021-33674, CVE-2021-33675 Product - SAP Contact Center, Version - 700	HotNews	9.6

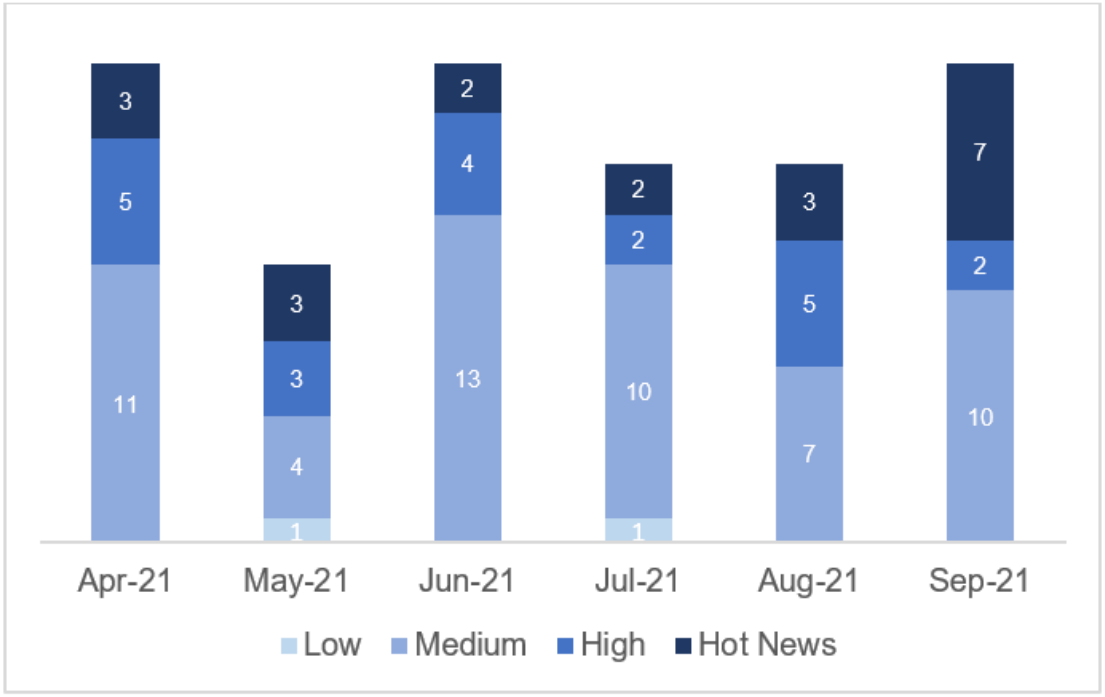
3080567	[CVE-2021-38162] **HTTP Request Smuggling in SAP Web Dispatcher** Product - SAP Web Dispatcher , Versions - WEBDISP - 7.49, 7.53, 7.77, 7.81, KRNL64NUC - 7.22, 7.22EXT, 7.49, KRNL64UC -7.22, 7.22EXT, 7.49, 7.53, KERNEL - 7.22, 7.49, 7.53, 7.77, 7.81, 7.83	High	8.9
3051787	[CVE-2021-38177] **Null Pointer Dereference vulnerability in SAP CommonCryptoLib** Product - SAP CommonCryptoLib , Versions - 8.5.38 or lower	High	7.5
3069032	[CVE-2021-33685] **Directory Traversal vulnerability in SAP Business One** Product - SAP Business One, Versions - 10.0	Medium	6.5
3082500	[CVE-2021-38175] **Information Disclosure in SAP Analysis for Microsoft Office** Product - SAP Analysis for Microsoft Office , Version - 2.8	Medium	6.5
3060621	[CVE-2021-38150] **Information disclosure in SAP Business Client** Product - SAP Business Client , Versions - 7.0, 7.70	Medium	6.1
3055180	[CVE-2021-33679] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence Platform (BI Workspace)** Product - SAP BusinessObjects Business Intelligence Platform (BI Workspace) , Version - 420	Medium	5.4
3068582	[CVE-2021-38164] **Missing Authorization check in in SAP ERP Financial Accounting / RFOPENPOSTING_FR** Product - SAP ERP Financial Accounting (RFOPENPOSTING_FR) , Versions - SAP_APPL - 600, 602, 603, 604, 605, 606, 616, SAP_FIN - 617, 618, 700, 720, 730, SAPSCORE - 125, S4CORE, 100, 101, 102, 103, 104, 105	Medium	5.4
3070138	[CVE-2021-33686] **Information Disclosure in SAP Business One** Product - SAP Business One, Version - 10.0	Medium	5.3
3082219	[CVE-2021-21489] **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	4.8
3069882	[CVE-2021-33688] **SQL Injection vulnerability in SAP Business One** Product - SAP Business One, Version - 10.0	Medium	4.3
3075546	[CVE-2021-37532] **Directory Listing Enabled in SAP Business One** Product - SAP Business One, Version - 10.0	Medium	4.3
3087791	[CVE-2021-38174] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** Product - SAP 3D Visual Enterprise Viewer, Version - 9.0	Medium	4.3

Vulnerability Type Distribution - September 2021



#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (April– September 2021)**



** 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 take a look at all Security Notes published or updated after August 10, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'August 11, 2021 - September 14, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – October 2021

Created by Risham Guram on Oct 12, 2021

This post by SAP Product Security Response Team 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.*

On 12th of October 2021, SAP Security Patch Day saw the release of 13 Security Notes. There was 1 update to previously released Patch Day Security Note.

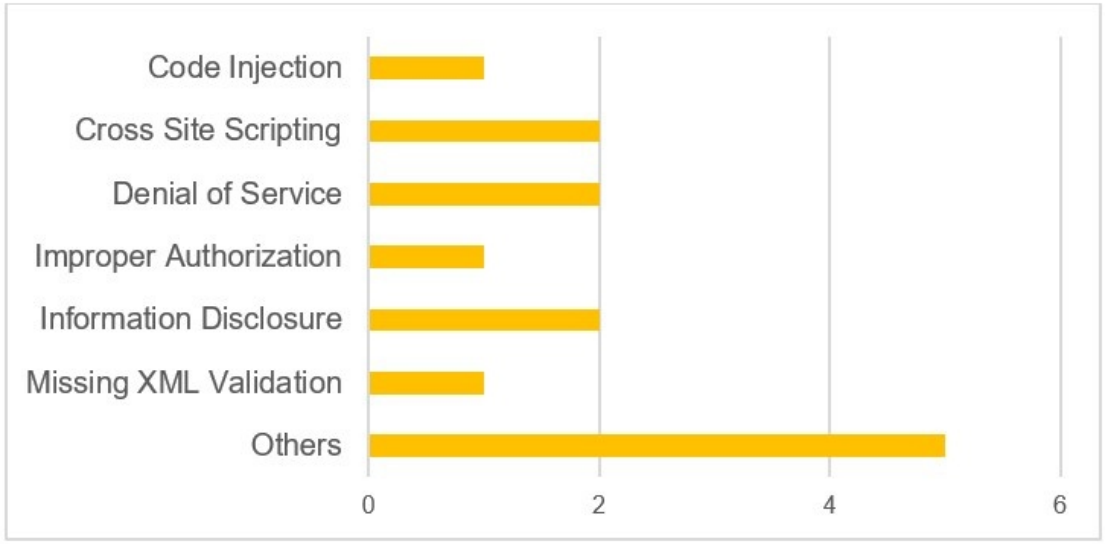
List of security notes released on October Patch Day:

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	HotNews	10
3101406	**Potential XML External Entity Injection Vulnerability in SAP Environmental Compliance** Related CVEs - CVE-2020-10683, CVE-2021-23926 Product - SAP Environmental Compliance, Version - 3.0	HotNews	9.8
3097887	[CVE-2021-38178] **Improper Authorization in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 701, 702, 710, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756	HotNews	9.1
3077635	[CVE-2021-40498] **Denial of service (DOS) in the SAP SuccessFactors Mobile Application for Android devices** Product - SAP SuccessFactors Mobile Application (for Android devices), Versions - <2108	High	7.8
3074693	[CVE-2021-40500] **Missing XML Validation in SAP BusinessObjects Business Intelligence Platform (Crystal Reports)** Product - SAP BusinessObjects Business Intelligence Platform (Crystal Reports), Versions - 420, 430	Medium	6.9
3074819	[CVE-2021-38179] **Information Disclosure in SAP Business One** Product - SAP Business One, Version - 10.0	Medium	6.7

3079427	[CVE-2021-38180] **CSV Injection in SAP Business One** Product - SAP Business One, Version - 10.0	Medium	6.5
3080710	[CVE-2021-38181] **Denial of service (DOS) in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756	Medium	6.5
3100882	[CVE-2021-40499] **Code Injection vulnerability for SAP NetWeaver Application Server for ABAP (SAP Cloud Print Manager and SAPSprint)** Product - SAP NetWeaver Application Server for ABAP (SAP Cloud Print Manager and SAPSprint), Versions - 7.70, 7.70 PI, 7.70BYD	Medium	6.4
3055347	**Cross-Site Scripting (XSS) vulnerability in SAPUI5** Related CVE - CVE-2020-11023 Product - SAPUI5, Versions - 750, 753, 754	Medium	6.1
3084937	[CVE-2021-38183] **Cross-Site Scripting (XSS) vulnerability in cms Service of SAP NetWeaver** Product - SAP NetWeaver, Versions - 700, 701, 702, 730	Medium	5.4
3099011	[CVE-2021-40495] **Denial of Service (DOS) in SAP NetWeaver Application Server for ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 740, 750, 751, 752, 753, 754, 755	Medium	5.3
3098917	[CVE-2021-40497] **Information Disclosure in SAP BusinessObjects Analysis (edition for OLAP)** Product - SAP BusinessObjects Analysis, (edition for OLAP), Versions - 420, 430	Medium	4.3
3087254	[CVE-2021-40496] **Improper Access Control in SAP NetWeaver AS ABAP and ABAP Platform** Product - SAP NetWeaver AS ABAP and ABAP Platform, Versions - 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 785	Medium	4.3

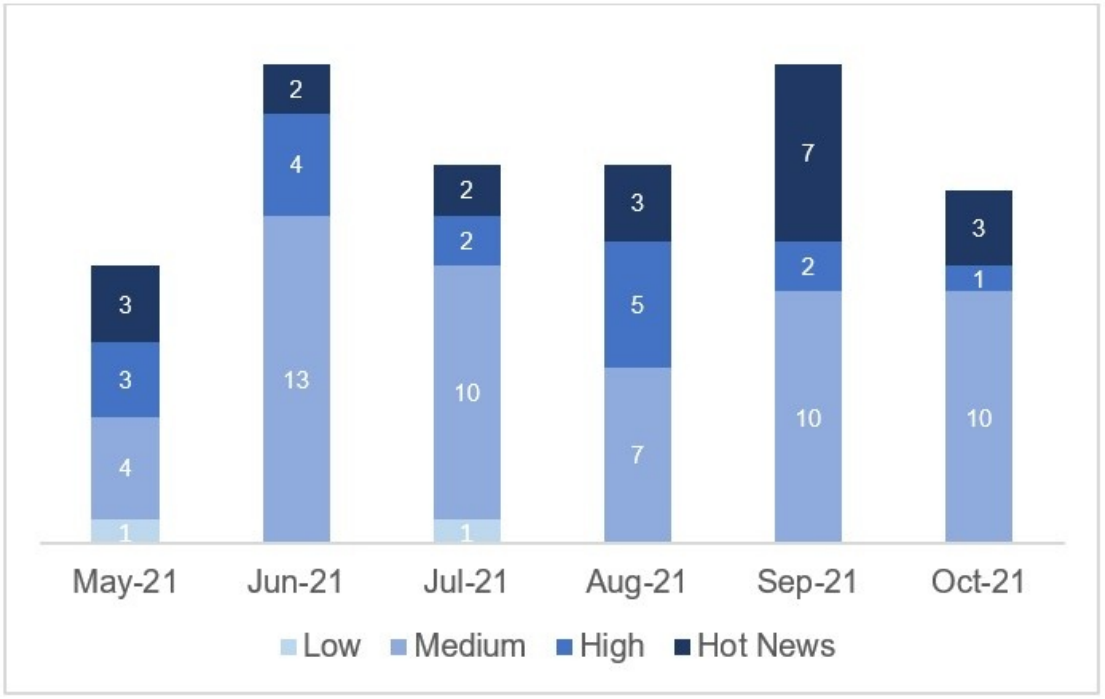
’ _____

Vulnerability Type Distribution - October 2021



#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (May – October 2021)**



** 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 take a look at all Security Notes published or updated after September 14, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'September 15, 2021 - October 12, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day – November 2021

Created by Risham Guram on Nov 09, 2021

This post by SAP Product Security Response Team 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.*

On 9th of November 2021, SAP Security Patch Day saw the release of 5 Security Notes. There were 2 updates to previously released Patch Day Security Notes.

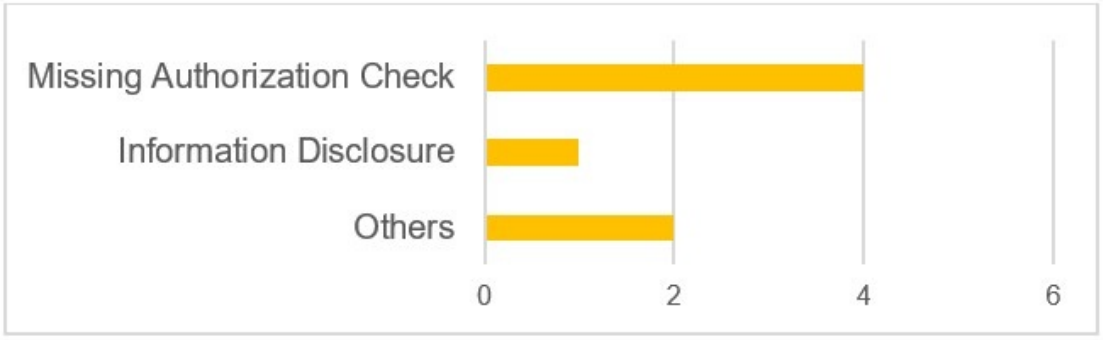
List of security notes released on November Patch Day:

Note#	Title	Priority	CVSS
3099776	[CVE-2021-40501] **Missing Authorization check in ABAP Platform Kernel** Product - SAP ABAP Platform Kernel, Versions - 7.77, 7.81, 7.85, 7.86	Hot News	9.6
3110328	[CVE-2021-40502] **Missing Authorization check in SAP Commerce** Product - SAP Commerce, Versions - 2105.3, 2011.13, 2005.18, 1905.34	High	8.3
2971638	***Update to Security Note released on October 2020 Patch Day:*** [CVE-2020-6369] **Hard-coded Credentials in CA Introscope Enterprise Manager (Affected products: SAP Solution Manager and SAP Focused** Product- CA Introscope Enterprise Manager (Affected products: SAP Solution Manager and SAP Focused Run), Versions - 9.7, 10.1, 10.5, 10.7	High	7.5
3080106	[CVE-2021-40503] **Information Disclosure in SAP GUI for Windows** Product - SAP GUI for Windows, Versions - < 7.60 PL13, 7.70 PL4	Medium	6.8
3104456	[CVE-2021-42062] **Missing Authorization check in SAP ERP HCM** Product - SAP ERP HCM Portugal, Versions - 600, 604, 608	Medium	6.5

3068582	***Update to Security Note released on September 2021 Patch Day:*** [CVE-2021-38164] **Missing Authorization check in in SAP ERP Financial Accounting / RFOPENPOSTING_FR** Product - SAP ERP Financial Accounting (RFOPENPOSTING_FR) , Versions - SAP_APPL - 600, 602, 603, 604, 605, 606, 616, SAP_FIN - 617, 618, 700, 720, 730, SAPSCORE - 125, S4CORE, 100, 101, 102, 103, 104, 105	Medium	5.4
3105728	[CVE-2021-40504] **Leverage of Permission in SAP NetWeaver Application Server for ABAP and ABAP Platform** Product - SAP NetWeaver AS for ABAP and ABAP Platform, Versions - 700, 701, 702,710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756	Medium	4.9

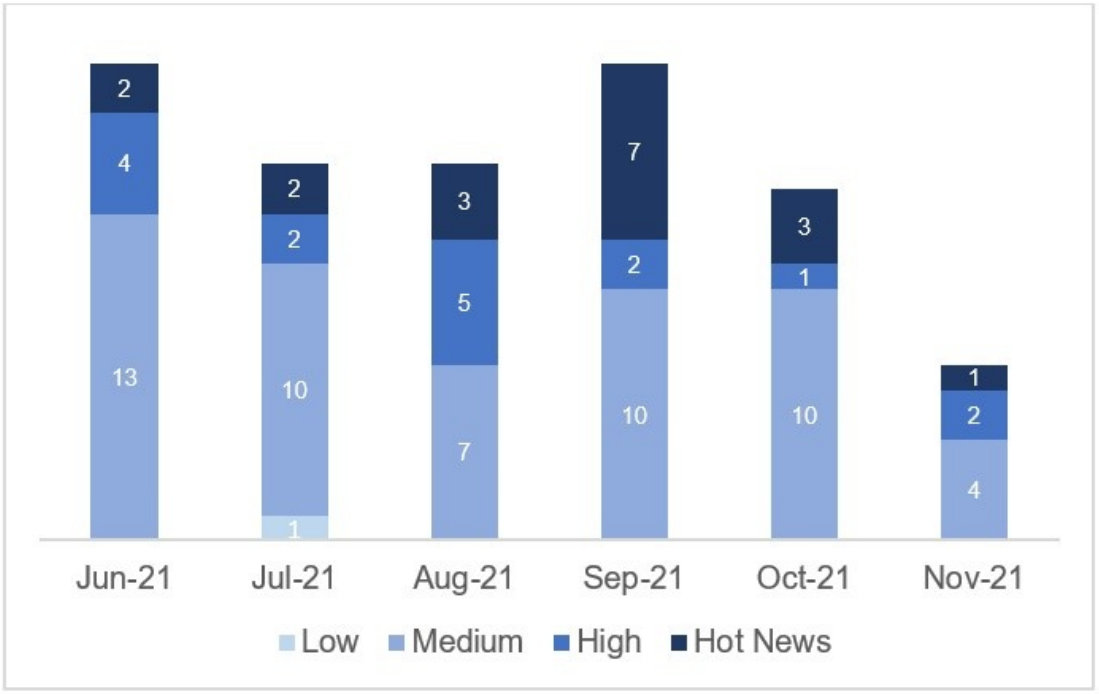
, _____

Vulnerability Type Distribution - November 2021



#*Multiple vulnerabilities on same product can be fixed by one security note.*

Security Notes vs Priority Distribution (June – November 2021)**



** 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 take a look at all Security Notes published or updated after October 12, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'October 13, 2021 - November 9, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels

SAP Security Patch Day - December 2021

Created by Risham Guram, last modified by Aditi Kulkarni on Feb 11, 2022

This post by SAP Product Security Response Team 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.*

On 14th of December 2021, SAP Security Patch Day saw the release of 11 Security Notes. There were 5 updates to previously released Patch Day Security Notes. Read SAP's statement on CVE-20211-44228 here.

List of security notes released on December Patch Day:

Note#	Title	Priority	CVSS
2622660	***Update to Security Note released on 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
3109577	**Code Execution vulnerability in SAP Commerce, localization for China** Related CVEs - CVE-2021-21341,CVE-2021-21342,CVE-2021-21349,CVE-2021-21343,CVE-2021-21344,CVE-2021-21346,CVE-2021-21347,CVE-2021-21350,CVE-2021-21351,CVE-2021-21345,CVE-2021-21348 Product - SAP Commerce, localization for China, Version - 2001	Hot News	9.9
3119365	[CVE-2021-44231] **Code Injection vulnerability in SAP ABAP Server & ABAP Platform (Translation Tools)** Product - SAP ABAP Server & ABAP Platform (Translation Tools), Versions - 701, 740,750,751,752,753,754,755,756,804	Hot News	9.9
3089831	***Update to Security Note released on September 2021 Patch Day:*** [CVE-2021-38176] **SQL Injection vulnerability in SAP NZDT Mapping Table Framework** Product - SAP S/4HANA, Versions - 1511, 1610, 1709, 1809, 1909, 2020, 2021 Product - SAP LT Replication Server, Versions - 2.0, 3.0 Product - SAP LTRS for S/4HANA, Version - 1.0 Product - SAP Test Data Migration Server, Version - 4.0 Product - SAP Landscape Transformation, Version - 2.0	Hot News	9.9
3114134	[CVE-2021-42064] **SQL Injection vulnerability in SAP Commerce** Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011	High	8.8
3102769	[CVE-2021-42063] **Cross-Site Scripting (XSS) vulnerability in SAP**	High	8.8

	Knowledge Warehouse Product - SAP Knowledge Warehouse, Versions - 7.30, 7.31, 7.40, 7.50		
3123196	[CVE-2021-44235] **Code Injection vulnerability in utility class for SAP NetWeaver AS ABAP** Product - SAP NetWeaver AS ABAP, Versions - 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756	High	8.4
3077635	[CVE-2021-40498] **Denial of service (DOS) in the SAP SuccessFactors Mobile Application for Android devices** Product - SAP SuccessFactors Mobile Application (for Android devices), Versions - <2108	High	7.8
3124094	[CVE-2021-44232] **Directory Traversal vulnerability in SAF-T Framework** Product - SAF-T Framework, Versions - SAP_FIN 617, 618, 720, 730, SAP_APPL 600, 602, 603, 604, 605, 606, S4CORE 102, 103, 104, 105	High	7.7
3113593	**Denial of service (DOS) in SAP Commerce** Related CVE - CVE-2021-37714 Product - SAP Commerce, Versions - 1905, 2005, 2105, 2011	High	7.5
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
3121165	[Multiple CVEs] **Improper Input Validation in SAP 3D Visual Enterprise Viewer** CVEs - CVE-2021-42068,CVE-2021-42070, CVE-2021-42069, CVE-2021-42069 Product - SAP 3D Visual Enterprise Viewer, Version - 9	Medium	4.3
2843016	***Update to Security Note released on November 2019 Patch Day:*** [CVE-2019-0388] **Content spoofing vulnerability in UI5 HTTP Handler** Product - SAP UI, Versions - 7.5, 7.51, 7.52, 7.53, 7.54 Product - SAP UI 700, Versions - 2.0	Medium	4.3
3103677	[CVE-2021-42061] **Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Business Intelligence platform (Web Intelligence)** Product - SAP BusinessObjects Business Intelligence Platform, Version - 420	Medium	4.1
3080816	[CVE-2021-44233] **Missing Authorization check in GRC Access Control** Product - SAP GRC Access Control, Versions - V1100_700, V1100_731,	Low	2.4

	V1200_750		

Note: Graphs could not be added due to an issue in the editor.

Customers who would like to take a look at all Security Notes published or updated after November 9, 2021, go to Launchpad Expert Search → Filter 'SAP Security Notes' released between 'November 10, 2021 - December 14, 2021' → Go.

To know more about the security researchers and research companies who have contributed for security patches of this month, visit SAP Product Security Response Acknowledgement Page.

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

SAP Product Security Response Team

No labels