LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

November 2018

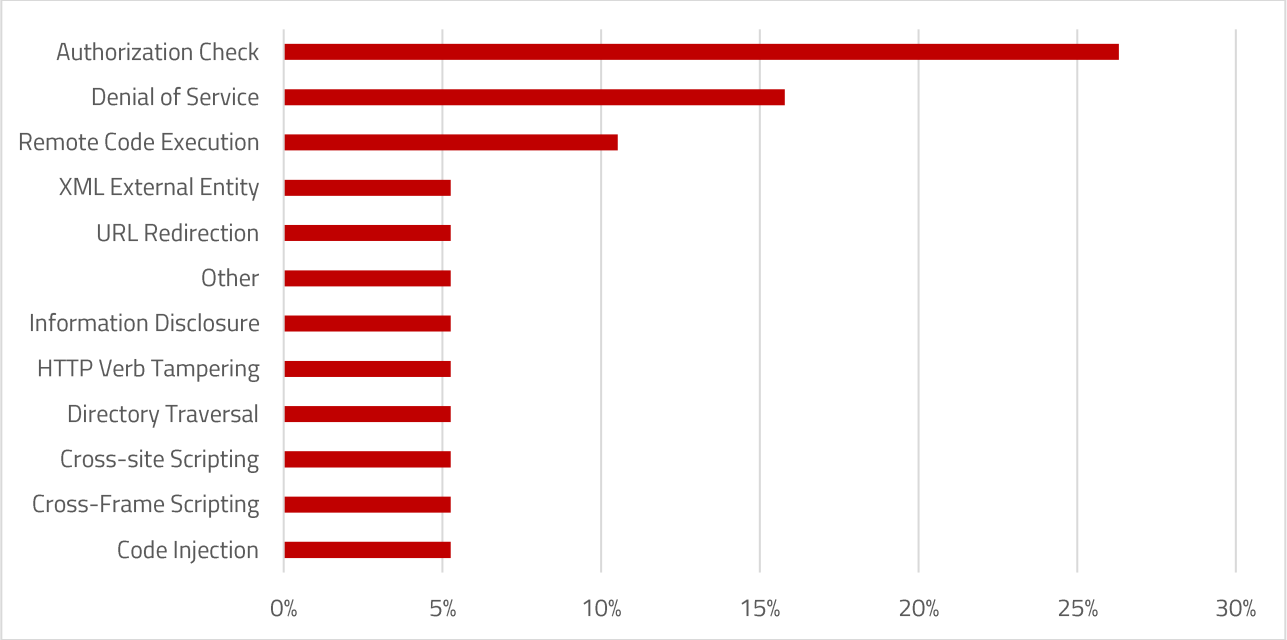
SAP Security Notes

November 2018

Hot News Note 2622660 includes critical security updates for web browser controls delivered with SAP Business Client. The Client provides a unified environment for SAP applications including Fiori, SAP GUI, and Web Dynpro. It supports browser controls from Internet Explorer (IE) and Chrome for displaying HTML content. Security corrections for the WebBrowser control of the .NET framework in IE are delivered directly by Microsoft. Unlike IE, the browser control for Chrome is embedded in SAP Business Client using the open source Chromium Embedded Framework (CEF). Security fixes are provided by the Chromium project and delivered by SAP through periodic Security Notes. Note 2622660 was updated for multiple high-risk vulnerabilities addressed by Chromium release 70.0.3538.

Note 2681280 patches a critical remote code execution vulnerability in SAP HANA Streaming Analytics (HSA). The vulnerability impacts the open source Java-based Spring Framework library used by HSA. The note carries a CVSS score of 9.9/10.

Note 2701410 deals with a high-risk directory traversal vulnerability that could be exploited by attackers to access, modify or corrupt files on hosts supporting SAP Disclosure Management.



SAP Security Notes by Vulnerability Type

Note 2693083 removes transaction ZPTTNO_TIME from the standard role SAP_PS_RM_PRO_RECMANAGER. The transaction could be abused to escalate privileges in CRM Records and Case Management.

Appendix: SAP Security Notes, November 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for the browser control Chromium delivered with SAP Business Client
HOT NEWS	2681280	HAN-SDS	Security vulnerability in Spring Framework library used by SAP HANA Streaming Analytics
HIGH	2701410	EPM-DSM-GEN	[CVE-2018-2487] Zip Slip in SAP Disclosure Management
HIGH	2693083	CA-GTF-RCM	[CVE-2018-2481] Leveraging privileges by customer transaction code
HIGH	2691126	MOB-FC	[CVE-2018-2485] Security vulnerabilities in SAP Fiori Client
HIGH	2657670	BI-RA-WBI-BE	[CVE-2018-2473] Denial of service (DOS) in Web Intelligence Richclient 3 Tiers Mode
MEDIUM	2197830	FS-AM	Missing authorization check in Account Management
MEDIUM	2061129	FIN-FSCM-DM	Missing whitelist check in SAP Dispute Management
MEDIUM	2028904	BC-MID-ICF-LGN	Cross-Frame Scripting protection in SAP ABAP HTTP logon application
MEDIUM	2272676	BC-WD-CMP-ALV-ABA	Spreadsheet Formula Injection in FPM List UIBB ATS/FPM Tree UIBB/WD ALV
MEDIUM	2671160	BC-CTS-TMS	[CVE-2018-2441] Missing input validation in ABAP Change and Transport System (CTS)
MEDIUM	2530147	IS-DFS-MM-STO	Missing Authorization check in DFPS stock transfer process
MEDIUM	2661740	EP-KM-TLS-XFB	[CVE-2018-2477] XML External Entity (XXE) vulnerability in SAP NetWeaver Knowledge Management XMLForms
MEDIUM	2490973	SRM-EBP-INT	Missing Authorization check in SAP SRM
MEDIUM	2676094	BI-BIP-BIW	[CVE-2018-2479] Cross-site Scripting vulnerability in BIWorkspace
MEDIUM	2675696	BC-TRX-API	[CVE-2018-2478] Remote Code Execution on TREX/BWA
MEDIUM	2647714	BI-BIP-CMC	[CVE-2018-2483] HTTP Verb Tampering vulnerability in SAP BI CMC
MEDIUM	2695896	MOB-SEC	[CVE-2018-2482] Denial of Service (DoS) in SAP Mobile Secure Android Application
MEDIUM	2658755	BC-COM-FOR	[CVE-2018-2476] URL Redirection vulnerability in "Forums in SAP NetWeaver"

LAYER SEVEN SECURITY

Layer Seven Security serve customers worldwide to secure, patch and monitor SAP systems against cyber threats using SAP Solution Manager

Address

99 Hudson Street
5th Floor
New York, NY 10013
United States

Web

www.layersevensecurity.com

Email

info@layersevensecurity.com

Telephone

1-647-964-7370