LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

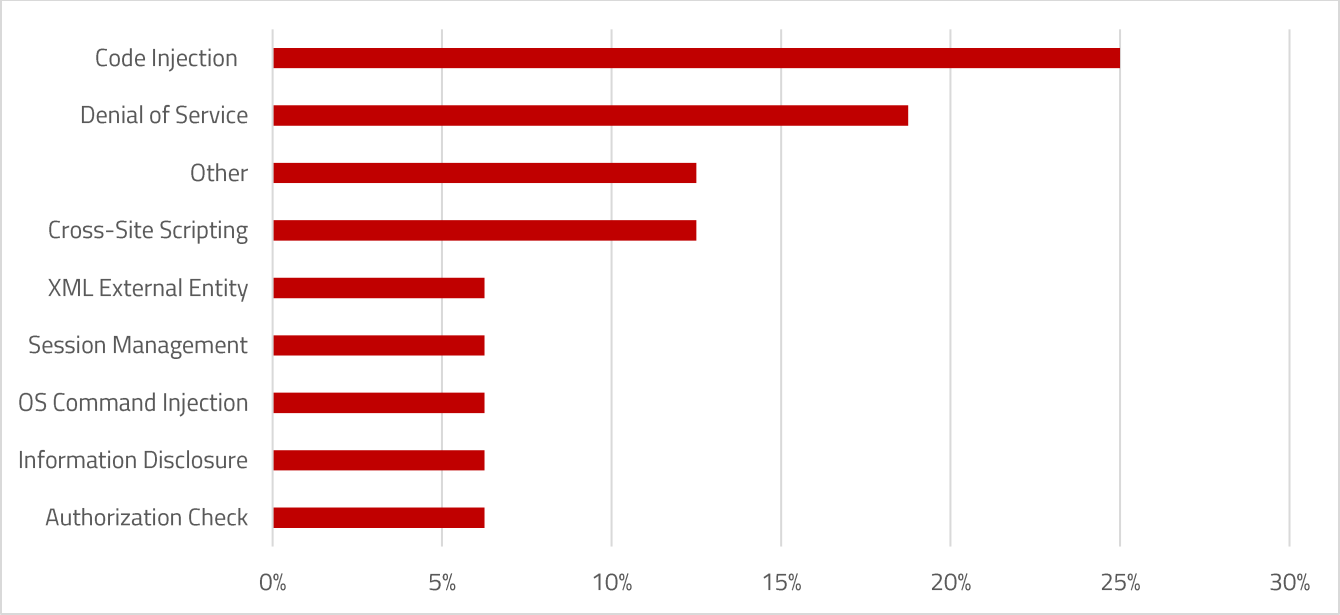
May 2018

SAP Security Notes

May 2018

SAP released an update for Hot News Note 2357141 which addresses a critical OS command injection vulnerability in the terminology export report program of SAPterm (transaction STERM). STERM is used to search SAP-delivered terminology and create and maintain customer-specific terminology. TERM_EXCEL_EXPORT is a standard executable program that enables users to export terminology repositories to Excel. The program calls function modules that accept unfiltered user commands in expressions that are used to call systems. This could be abused by attackers perform arbitrary operating system commands using the elevated privileges of the <sid>adm user. The impact of such an exploit could include compromise of the entire SAP file system in the effected host. This explains the high CVSS base score of 9.1 / 10 for Note 23557141. The Note rates high in terms of the impact to information confidentiality, integrity and availability. Systems with SAP_BASIS versions 7.31 – 7.66 should be patched to the relevant Support Package level listed in the Note.

There was also an important update for Note 2622660 which 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.



SAP Security Notes by Vulnerability Type

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 includes corrections addressed by Chromium releases 64 and 65. The critical rating of the note is due to the fact that the highest CVSS rating of the security corrections bundled in the fixes is 9.8/10.

Finally, Note 2537150 was re-released with updated support pack information. The Note includes corrections to automatically terminate active sessions for users whose passwords have been changed in BusinessObjects.

Appendix: SAP Security Notes, May 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2357141	BC-DOC-TER	OS Command Injection vulnerability in Report for Terminology Export
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for 3rd party web browser controls delivered with SAP Business Client
HIGH	2537150	BI-BIP-INV	[CVE-2018-2408] Improper Session Management in SAP Business Objects - CMC/BI Launchpad/Fiorified BI Launchpad
MEDIUM	2634240	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2638709	OPU-GW-JAV	Code Injection vulnerability in SAP HCI TOOLS
MEDIUM	2597875	BC-IAM-IDM	[CVE-2018-2416] Missing XML Validation vulnerability in SAP Identity Management
MEDIUM	1999142	BI-RA-CR	Potential remote code execution in BI-RA-CR
MEDIUM	2550202	BC-JAS-WEB	[CVE-2018-2415] Content Spoofing Vulnerability in NetWeaver Java AS Web Container and HTTP Service
MEDIUM	2620744	BC-FES-IGS	[CVE-2018-2423] Denial of Service in SAP Internet Graphic Server (IGS) RFC listener
MEDIUM	2610231	BC-DB-SDB-DBA	[CVE-2018-2418] Code Injection Vulnerability in SAP MaxDB ODBC Driver
MEDIUM	2617553	BC-FES-IGS	[CVE-2018-2422] Denial of Service in SAP Internet Graphic Server (IGS) Portwatcher
MEDIUM	2616599	BC-FES-IGS	[CVE-2018-2421] Denial of Service in SAP Internet Graphics Server (IGS) Portwatcher
MEDIUM	2615635	BC-FES-IGS	[CVE-2018-2420] Unrestricted File Upload in SAP Internet Graphics Server (IGS)
MEDIUM	2601492	BC-IAM-IDM	[CVE-2018-2417] Information Disclosure in SAP Identity Management Runtime component
MEDIUM	2588567	CA-WUI-UI-TAG	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
LOW	2596627	IS-B-BCA-MD	[CVE-2018-2419] Missing Authorization check in SAP Enterprise Financial Services

LAYER SEVEN SECURITY

Layer Seven Security serve customers worldwide to harden, 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