LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

June 2018

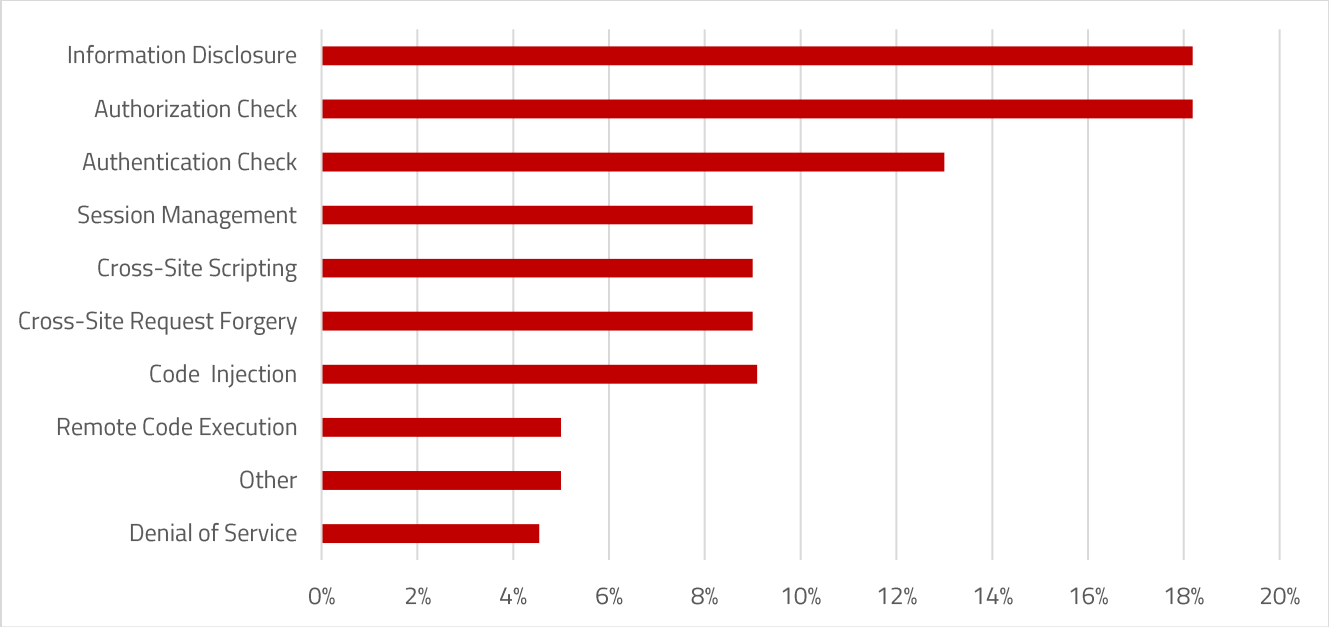
SAP Security Notes

June 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 in June for corrections addressed by Chromium release 67.0.3396. 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.

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

Notes 2629535 and 2626762 patch high-risk vulnerabilities in open-source components bundled in SAP Internet Sales. The vulnerabilities could be exploited to provoke a denial of service or bypass authentication and authorization controls. SAP Internet Sales is often tightly integrated with back-end SAP systems for order fulfillment and processing.



SAP Security Notes by Vulnerability Type

Finally, there were several important notes released for SAP Solution Manager. Note 2546807 provides manual instructions for successfully connecting agents for Wily Introscope to managed systems. Introscope is included in Solution Manager to support diagnostics and monitoring. Note 2574394 includes steps for authenticating and encrypting connections from Solution Manager to Diagnostics Agents using TLS. Instructions for securing connections from Diagnostics Agents to Solution Manager are available in Note 2593479.

Appendix: SAP Security Notes, June 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for 3rd party web browser controls delivered with SAP Business Client
HIGH	2604054	CA-GTF-PWB	Missing Authorization check in Printworkbench
HIGH	2546807	SV-SMG-INS-CFG-MNG	List of Diagnostic Agents can't be retrieved due to enforced security at API level
HIGH	2537150	BI-BIP-INV	[CVE-2018-2408] Improper Session Management in SAP Business Objects - CMC/BI Launchpad/Fiorified BI Launchpad
HIGH	2629535	CRM-ISA-TEC	Denial of service (DOS) in Internet Sales
HIGH	2626762	CRM-ISA	Code Injection vulnerability in SAP Internet Sales
HIGH	2588475	SBO-CRO-SEC	[CVE-2018-2425] Information Disclosure in SAP Business One for SAP HANA Backup Service
MEDIUM	2610231	BC-DB-SDB-DBA	[CVE-2018-2418] Code Injection Vulnerability in SAP MaxDB ODBC Driver
MEDIUM	2658149	FI-FIO-AR	Cross-Site Request Forgery (CSRF) vulnerability in F2626 and F1680
MEDIUM	2662632	FI-FIO-AR	Cross-Site Request Forgery (CSRF) vulnerability in F0744
MEDIUM	2518906	BI-RA-CRE-VIE	Vulnerability in Crystal Reports web viewers
MEDIUM	1999142	BI-RA-CR	Potential remote code execution in SAP CrystalReports
MEDIUM	2110950	SV-SMG-SYS	Potential disclosure of persisted data in ST
MEDIUM	1900259	SV-SMG	Potential disclosure of persisted data in AI_SBUSDOC
MEDIUM	1553387	SV-SMG	Violation of PIL 2.0 Security Standard Requirement
MEDIUM	2574394	SV-SMG-DIA-SRV-AGT	Configure Diagnostics Agents to Check the Solution Manager Server Certificate
MEDIUM	2473452	FS-CMS-MD	Missing Authorization check in FS-CMS
MEDIUM	2538856	CA-UI5-CTR-ROD	[CVE-2018-2424] Cross-Site Scripting (XSS) vulnerability in SAPUI5
MEDIUM	2621121	CA-UI5-DLV	[CVE-2018-2428] Information Disclosure in UI5 Handler
MEDIUM	2546300	XX-PROJ-FI-CA	Switchable Authorization checks for RFC in FI-CA for Data Protection
LOW	2593479	SV-SMG-DIA-SRV-AGT	Checking server certificates and host name of managed systems
LOW	2638217	FI-CF-INF	Switchable Authorization Checks in Central Finance Infrastructure Components

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

© Copyright Layer Seven Security 2018 - All rights reserved.