LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

August 2018

SAP Security Notes

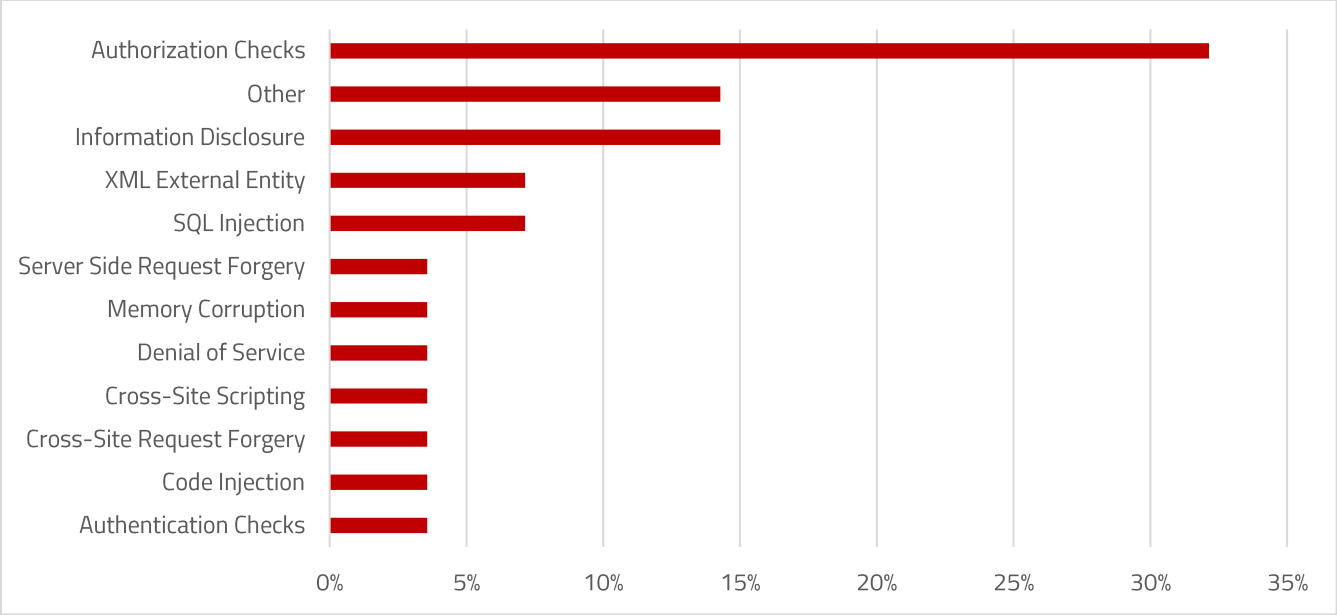
August 2018

There were several high priority Security Notes released in August for vulnerabilities impacting multiple Business Intelligence applications. Note 2569748 patches an XML External Entity vulnerability in Crystal Reports for Enterprise. Note 2614229 deals with a memory corruption vulnerability in the BOBJ platform that can be triggered by a buffer overflow. Note 2644154 provides corrections for a SQL injection vulnerability in the BI Launchpad for Web Intelligence that could be exploited to read sensitive data.

A similar SQL injection vulnerability is addressed in the MaxDB database by note 2660005. The solution includes removing unnecessary privileges for DBM operators responsible for managing databases.

Notes 2655250 and 2155614 patch missing authorization checks in the MDM Catalog of Supplier Relationship Management (SRM) and components of ERP Sales and Distribution.

Note 2201710 includes instructions for responding to Logjam and similar vulnerabilities in SAP products using OpenSSL. Logjam involves downgrading vulnerable TLS connections using ephemeral Diffie-Hellman key exchange to 512-bit export-grade cryptography. Note 2201710 adds protection for TLS clients by rejecting handshakes with DH parameters shorter than 768 bits.



SAP Security Notes by Vulnerability Type

Appendix: SAP Security Notes, August 2018 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2622660	BC-FES-BUS-DSK	Security updates for the browser control Chromium delivered with SAP Business Client
HIGH	2569748	BI-RA-CRE	XML External Entity vulnerability in Crystal Reports for Enterprise
HIGH	2655250	SRM-CAT-MDM	[CVE-2018-2449] Missing Authentication check in SAP SRM MDM Catalog
HIGH	2614229	BI-RA-WBI-BE-DP	Memory Corruption vulnerability in SAP BusinessObjects Business Intelligence platform
HIGH	2644154	BI-RA-WBI-FE-HTM	[CVE-2018-2447] SQL Injection vulnerability in BI Launchpad Web Intelligence
HIGH	2621395	EPM-BFC-TCL	[CVE-2018-2444] Cross-Site Scripting (XSS) vulnerability in SAP Financial Consolidation
HIGH	2660005	BC-DB-SDB	[CVE-2018-2450] SQL Injection Vulnerability in SAP MaxDB/liveCache
HIGH	2155614	SD-SLS	Missing authorization check in SD-SLS, SD-CAS and SD-MD-AM-CMI
MEDIUM	2519562	XX-CSC-AR-LO	Missing Authorization check in XX-CSC-AR-LO
MEDIUM	2652186	BC-XI-CON-B2B	Denial of Service in B2B Adapters
MEDIUM	2201710	BC-SYB-PB	Fixing Logjam and Alternative chains certificate forgery vulnerabilities in multiple SAP products
MEDIUM	1640584	BC-MID-RFC	Missing authorization check for maintenance of trust
MEDIUM	2557167	BI-RA-CRE	Potential code injection vulnerability in Crystal Reports Java components
MEDIUM	2671160	BC-CTS-TMS	[CVE-2018-2441] Missing input validation in ABAP Change and Transport System (CTS)
MEDIUM	2653519	BC-IAM-IDM	[CVE-2018-2416] Missing XML Validation vulnerability in SAP Identity Management
MEDIUM	2590705	BC-XS-SEC	[CVE-2018-2451] Unsecure xs CLI session timeout handling in SAP HANA Extended Application Services, advanced
MEDIUM	2407193	BI-RA-WBI-FE-HTM	[CVE-2018-2442] Cross-Site Request Forgery (CSRF) in BI Launchpad Web Intelligence
MEDIUM	2633846	BI-BIP-QB	[CVE-2018-2446] Information disclosure vulnerability in BI Query Builder

Appendix: SAP Security Notes, August 2018 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2630018	BI-BIP-CMC	[CVE-2018-2445] Server Side Request Forgery (SSRF) vulnerability in SAP BusinessObjects BI Platform Servers AdminTools
MEDIUM	2653846	SRM-CAT-MDM	[CVE-2018-2448] Information Disclosure in SRM MDM Catalog
MEDIUM	2502878	LO-RFM-MD-QO	FM MD_SINGLE_ROUNDING should be RFC enabled and necessary authorization check done.
MEDIUM	2633180	CA-UI5-ABA-SAR	[CVE-2018-2434] Content Spoofing vulnerability in SAP_UI component
MEDIUM	2522527	SD-BIL	Switchable authorization checks for RFC of SD/FI-CA integration for distributed systems
MEDIUM	1951171	LO-SPM	Potentially controllable RFC function module for postings in EWM
MEDIUM	2030096	LO-SRS	Missing authorization check in component LO-SRS
MEDIUM	2030657	PSM-GPR	Switchable authorization checks for RFC in PSM-GPR
MEDIUM	1944155	CO-PA	Missing authorization check in report RKEDELE1
LOW	2638288	BW4-AE	Information Disclosure in OLAP Queries

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