LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

February 2018

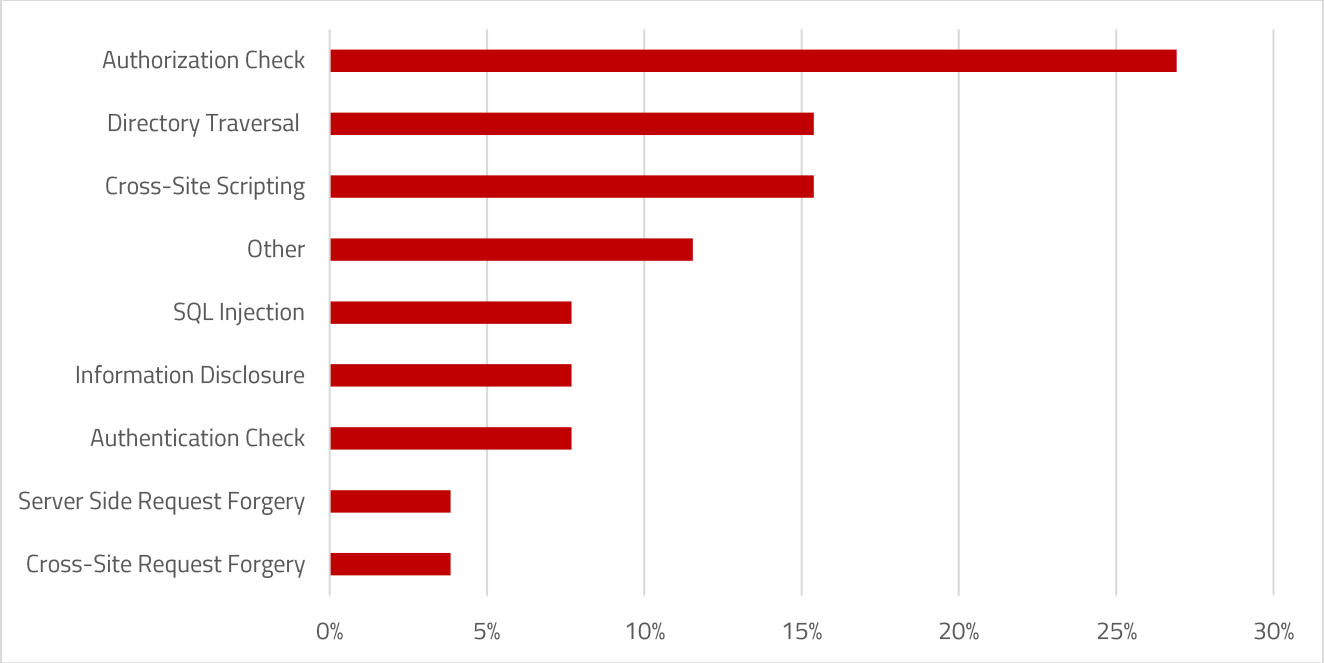
SAP Security Notes

February 2018

Note 2589129 addresses multiple high-risk vulnerabilities in HANA Extended Services Advanced (XSA) Server. XSA provides a development and runtime platform for HANA applications. XSA delivers improved reliability and scalability over HANA XS by providing separate runtime environments for applications. Applications operate in trust zones known as spaces. Applications deployed to the same space can share common resources such as data storage, user authorizations, and passwords. Permissions to manage spaces including domains and resources are granted through controller roles.

Note 2589129 recommends using HANA XSA patch level 1.0.70 in order to remove several authentication and authorization bypass vulnerabilities listed in the Note. This includes flaws in specific controller roles that could enable users to retrieve sensitive information. It also includes vulnerabilities that could enable unauthenticated or unauthorized users to read the system configuration using SQL statements and retrieve passwords from log files.

Note 2525222 includes automated corrections and manual instructions for high priority vulnerabilities in the SAP Internet Graphics Server (IGS). The vulnerabilities are caused by unrestricted file uploads that could be exploited to



SAP Security Notes by Vulnerability Type

provoke a denial of service, perform cross-site scripting or log injection attacks, and leak sensitive data.

Lastly, Note 2565622 includes corrections to remove a broken authentication vulnerability that could enable attackers to access privileged functions or read and modify sensitive data in the SAP NetWeaver System Landscape Directory (SLD). The SLD supports landscape management and stores destination information used for system interfaces and the NetWeaver Development Infrastructure (NWDI).

Appendix: SAP Security Notes, February 2018 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2589129	BC-XS-RT	[CVE-2018-2374] Security vulnerabilities in SAP HANA Extended Application Services, advanced
HIGH	2565622	BC-CCM-SLD	[CVE-2018-2368] Missing Authentication check in SAP NetWeaver System Landscape Directory
HIGH	2525222	BC-FES-IGS	[CVE-2018-2395] Security vulnerabilities in SAP Internet Graphics Server (IGS)
HIGH	1584573	BC-UPG	Security verdict in SUGM SAUS SUGM_UPG_TYPE_PLUS_DEL_XML
HIGH	1977547	BC-UPG-TLS-TLA	Update 1 to Security Note 1584573
MEDIUM	2473452	FS-CMS-MD	Missing Authorization check in FS-CMS
MEDIUM	1696317	CRM-ANA-PS	Unauthorized modification of displayed content in CRM-ANA-PS
MEDIUM	2536422	LO-MD-BP-CM	Information Disclosure in Customer factsheet
MEDIUM	2572940	HAN-DB-SEC	[CVE-2018-2369] Information Disclosure in authentication function of SAP HANA
MEDIUM	2531131	FI-CAX-FS	Switchable Authorization checks for RFC BCA_DIM_WRITE_OFF in Loans (FI-CAX-FS)
MEDIUM	2458919	PA-ER	Missing Authorization check in HCM E-recruiting
MEDIUM	2174147	IS-OIL-PRA-REP	Directory Traversal vulnerability in IS-OIL-PRA-REP-TAX and IS-OIL-PRA-REP-ROY
MEDIUM	1974016	BW-SYS-DB-DB4	Missing authorization check in function modules of BW-SYS-DB-DB4
MEDIUM	2592069	BC-DWB-AIE-SRC	Missing Authorization check in ABAP in Eclipse
MEDIUM	2562089	BC-ABA-LA	[CVE-2018-2367] Directory Traversal vulnerability in ABAP File Interface
MEDIUM	2560741	BC-JAS-SEC-SML	[CVE-2018-2371] Cross-Site Scripting (XSS) Vulnerability in SAML 2.0 Service Provider of AS Java
MEDIUM	2547977	BC-WD-JAV	[CVE-2018-2365] Cross-Site Scripting (XSS) vulnerability in SAP Netweaver Portal
MEDIUM	2547431	CRM-ISA	[CVE-2018-2380] Directory Traversal vulnerability in Internet Sales
MEDIUM	2545842	FI-GL-IS	[CVE-2018-2381] Missing Authorization check in SAP ERP Financials Information System
MEDIUM	2541700	CA-WUI-UI	[CVE-2018-2364] Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI

Appendix: SAP Security Notes, February 2018 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2493727	BI-BIP-INV	[CVE-2018-2370] Server Side Request Forgery(SSRF) vulnerability in Central Management Console, BI Launchpad and Fiori BI Launchpad
MEDIUM	1514066	BC-UPG	Overwriting files during upgrade or EHP installation
MEDIUM	2516864	QM	Missing authorization check in QM
MEDIUM	2494184	BC-SYB-SQA	Cross-Site Request Forgery (CSRF) vulnerability in multiple SAP Sybase products
LOW	2609847	FS-BA	DPP Blocking and Masking
LOW	2570335	CA-RT-CAR-OAA	OAA CDS Hardening

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