ADVISORY

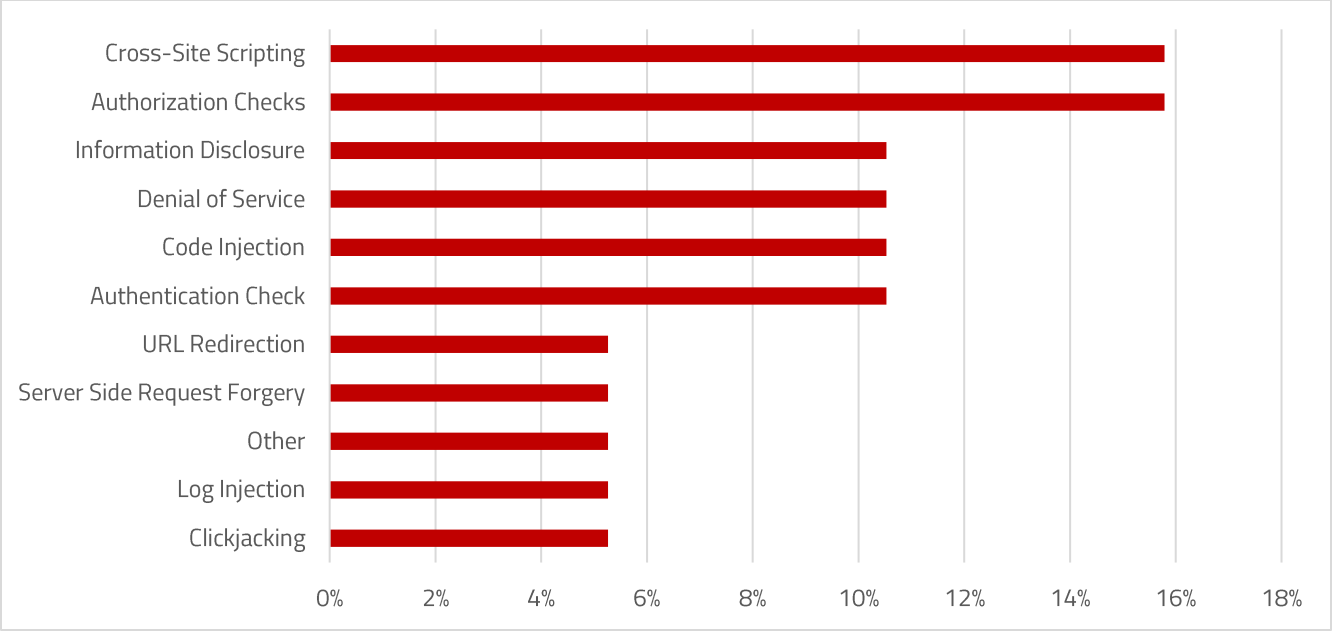
Layer Seven Security

SAP Security Notes

December 2017

Note 2449757 introduces an additional authentication check to improve security for trusted RFC connections. Trusted RFC is a method to establish secure RFC-based communication between systems and avoid the use of stored credentials in RFC destinations. Trust relationships are maintained using transaction SMT1 and provide the option to logon from trusted systems to trusting systems using the credentials of the current user in the trusted system. The trusting system performs a check for the authorization object S_RFCACL before permitting the connection. S_RFCACL includes several fields to restrict access from specific systems, clients, and transaction codes. However, the fields cannot be maintained in some scenarios such as central user management since users may require full S_RFCACL authorizations to access multiple systems in landscapes. This creates the risk that trusted connections could be exploited to perform client and user switches within systems. Internal RFC communications are trusted by default.

Note 2449757 delivers the new profile parameter rfc/selftrust to address the risk. Possible value settings for the parameter are 1 and 0. The default setting is 1 and is applied to trust all internal RFC communications. The value setting 0 only permits trusted internal RFC connections to different clients or users if the relationship is maintained in SMT1.



SAP Security Notes by Vulnerability Type

Note 2537152 patches a high priority missing authentication check in BI Promotion Management used to transfer content between systems.

Note 2522510 deals with a log injection vulnerability in HANA Extended Application Services (XS). The vulnerability arises from insufficient input validation in HTTP/REST endpoints of the controller service in HANA XS and could impact the integrity of audit logs written to log files. Audit logs written to syslog or database tables are not impacted.

Appendix: SAP Security Notes, December 2017

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2537152	BI-BIP-LCM	[CVE-2017-16684] Missing Authentication check in SAP BI Promotion Management Application
HIGH	2449757	BC-MID-RFC	[CVE-2017-16689] Additional Authentication check in Trusted RFC on same system
MEDIUM	2580258	MOB-APP-ERP-DSD	Missing Authorization check in SAP Direct Store Delivery
MEDIUM	2529480	MFG-PCO	[CVE-2017-16690] DLL preload attack possible on NwSapSetup and Installation self extracting program for SAP Plant Connectivity
MEDIUM	2462261	CEC-MKT-BF	Missing Authorization check in Hybris Marketing
MEDIUM	2286679	BC-WD-JAV	Whitelist Service API required for the Clickjacking Framing Protection in JAVA at the framework or application level
MEDIUM	2537545	BW-BEX-UDI	[CVE-2017-16685] Cross-Site Scripting (XSS) vulnerability in SAP BW Universal Data Integration
MEDIUM	2546220	BC-UPG-NA	[CVE-2017-16691] SNOTE: Digital signature verification along with note file extraction
MEDIUM	2531656	BI-BIP-SRV	[CVE-2017-16683] Denial of service (DOS) in SAP BusinessObjects Platform
MEDIUM	2552295	BC-CST-DP	Denial of service (DOS) in ABAP System's Dispatcher
MEDIUM	2549983	HAN-AS-XS	[CVE-2017-16687] Information Disclosure in SAP HANA XS classic user self-service
MEDIUM	2526781	BC-FES-ITS	[CVE-2017-16682] Code Injection vulnerability in SAP NetWeaver/ITS
MEDIUM	2523913	BI-BIP-LCM	[CVE-2017-16681] Cross-Site Scripting (XSS) vulnerability in BI Promotion Management Application
MEDIUM	2522510	BC-XS-RT	[CVE-2017-16680] Potential audit log injection vulnerability in SAP HANA XS Advanced
MEDIUM	2520995	BC-CST-STS	[CVE-2017-16679] URL Redirection vulnerability in Startup Service
MEDIUM	2457562	EP-KM-FWK-CF	[CVE-2017-16678] Server Side Request Forgery (SSRF) vulnerability in SAP NetWeaver Knowledge Management Configuration Service
MEDIUM	2174651	BC-XI-IBC	Potential information disclosure relating to PI Integration Directory
MEDIUM	2495144	FI-CF-INF	Switchable Authorization checks for RFC in Central Finance
LOW	2453871	BI-RA-AD	Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Design Studio

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