Layer Seven Security

ADVISORY

SAP Security Notes

February 2017

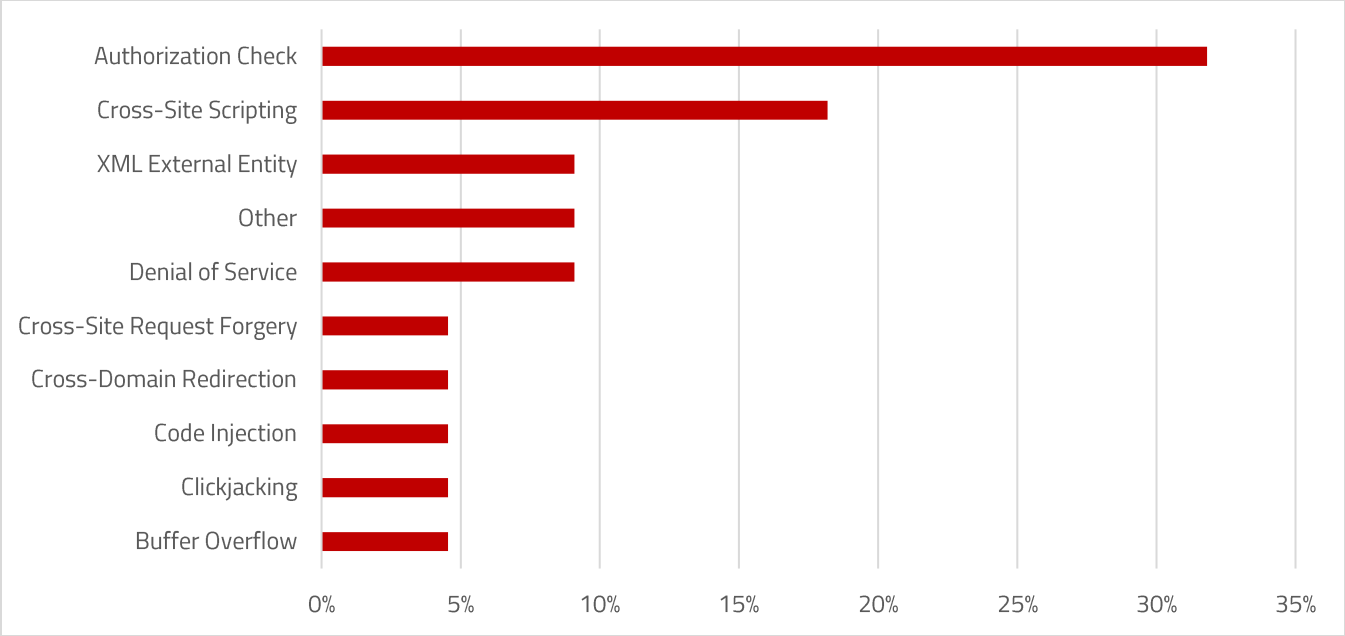
Note 2410061 patches a dangerous Distributed Denial of Service (DDoS) vulnerability in the Data Orchestration Engine (DOE) Administration Portal. The DOE is used to access the SAP NetWeaver Mobile Administrator to manage and monitor mobile system landscapes. This includes connecting mobile clients, deploying agents and packages to mobile devices, managing single sign-on, and other tasks.

The DDoS vulnerability stems from the system messages area of the DOE. This is used to transmit messages to mobile clients. Attackers can provoke a denial of service in the DOE by flooding the system messages service and exhausting available resources.

Note 2407694 addresses a similar denial of service vulnerability in the SAP Web IDE for SAP HANA. Web IDE is a development tool for building and deploying Fiori and other applications. The sinopia registry in the Web IDE crashes during publication if a package name contains special characters. Exploitation of the vulnerability can be prevented by blocking the registry from registering new users. The Note includes instructions for identifying systems that have been successfully attacked using the vulnerability. It also included details of a workaround to block attempted new user registrations by modifying permissions for the htpasswd file.

SAP Security Notes

February 2017



SAP Security Notes by Vulnerability Type

Note 2392860 removes the transaction code ZPTTNO_TIME from the standard roles SAP_PS_RM_PRO_ADMIN and SAP_PS_RM_PRO_REVIEWER. The transaction can be used to escalate privileges by creating other custom transactions.

Note 2413716 provides instructions for securing the trusted RFC connection for GRC Access Controls Emergency Access Management (EAM). The trusted connection is required to switch user accounts to Fire Fighter IDs (FFIDs).

The instructions include maintaining the authorization objects S_RFCACL and S_ICF, deactivating passwords for FFIDs, and controlling critical basis authorizations for managing trust relationships and RFC destinations.

Appendix: SAP Security Notes, February 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2408892	BC-MOB-DOE	Missing Authorization Checks in SAP Netweaver Data Orchestration Engine
HIGH	2410061	BC-MOB-DOE	Denial of service (DOS) in "System Messages" area in DOE Administration Portal
HIGH	2407694	HAN-WDE	SAP Web IDE for SAP HANA: Unauthorized remote data tampering and DOS attack
HIGH	2391018	CA-VE-VEV	Memory Corruption vulnerability in SAP 3D Visual Enterprise Author, Generator and Viewer
HIGH	2392860	BC-SRV-RM	Leveraging privileges by customer transaction code
HIGH	2278931	BC-SRV-KPR-DMS	Code injection vulnerability in BC-SRV-KPR-DMS
HIGH	2413716	GRC-SAC-EAM	Setup of Trusted RFC in GRC Access Control EAM
MEDIUM	2280932	BC-JAS-SEC-LGN	Missing authorization check in Security Service
MEDIUM	2367193	XX-CSC-RU-FI	Missing Authorization check in Cash Flow Statement report
MEDIUM	2350276	BC-FES-ITS	Cross-Site Scripting (XSS) vulnerability in ITS / SAP GUI for HTML
MEDIUM	2326291	EP-KM-CM-UI	Cross-Site Scripting (XSS) vulnerability in KM Portal Favorites
MEDIUM	2386873	BW-BEX-UDI-VC	Missing XML Validation vulnerability in Visual Composer VC70RUNTIME
MEDIUM	2369541	EP-PIN-IVS-UPL	Missing XML Validation vulnerability in Enterprise Portal
MEDIUM	2360489	EP-VC-CON	Cross-Site Request Forgery (CSRF) vulnerability in Visual Composer 04s iviews.
MEDIUM	2197532	BC-FES-ITS	Security vulnerabilities in an ICF service belonging to SAP ITS Mobile
MEDIUM	2408558	BC-CTS-ORG	Missing Authorization check in Transaction GTABKEY
MEDIUM	2401265	BC-CUS-TOL-IMG	Missing Authorization check in the FM OBJECT_MAINTENANCE_CALL
MEDIUM	2292351	BI-BIP-LCM	Cross-Site Scripting (XSS) vulnerability in SAP BI Promotion Management Application
MEDIUM	2319172	BC-FES-ITS	Whitelist based Clickjacking Framing Protection in SAP GUI for HTML
MEDIUM	2407845	BC-SYB-ASE	Multiple vulnerabilities when using JAVA in SAP ASE

Appendix: SAP Security Notes, February 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2250817	BI-BIP-INV	Cross-Site Scripting (XSS) vulnerability in Infoview - Titan
LOW	2185122	CA-MDG-APP-FIN	Switchable authorization checks for RFC in data extraction within CA-MDG-APP-FIN

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