ADVISORY

Layer Seven Security

SAP Security Notes

May 2017

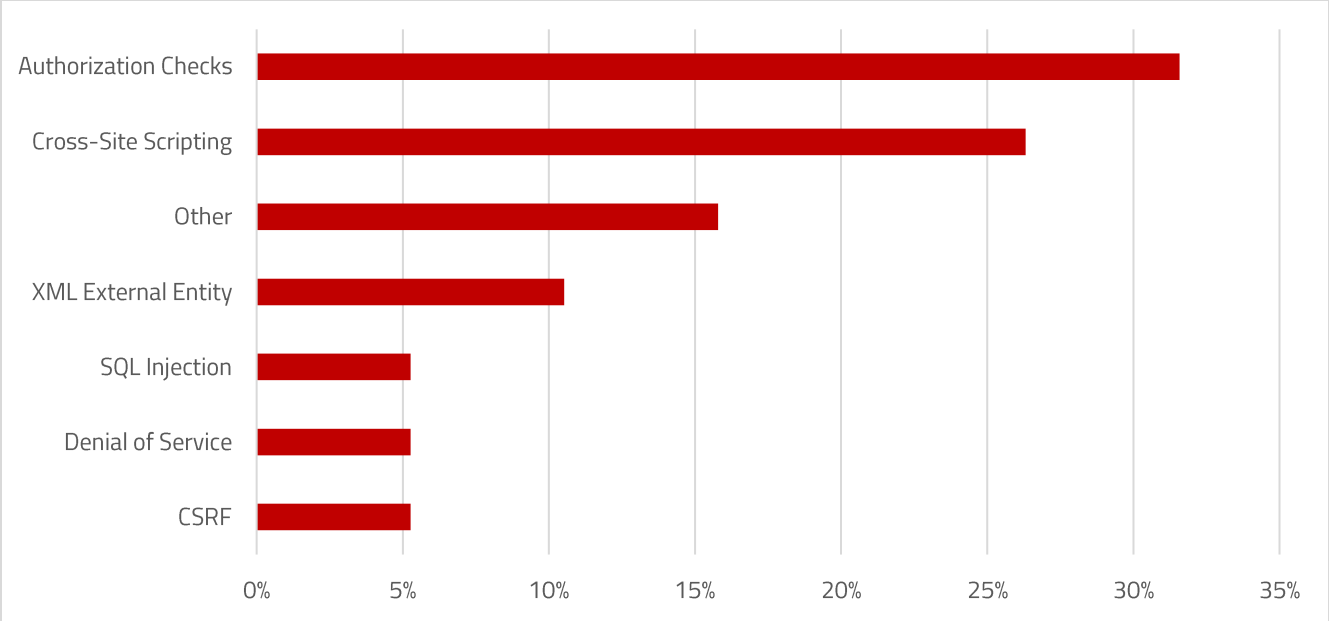
SAP Security Notes

May 2017

Note 2380277 addresses a high priority memory corruption vulnerability in the GUI control component of the Internet Graphics Server (IGS). GUI control is a self-contained component of the presentation server in ABAP systems. The Note contains corrections for logical errors in memory management within the component. The errors could be exploited by attackers to extract sensitive information or perform a denial of service by provoking a buffer overflow or underflow. This is caused by specially crafted commands or objects that force GUI Control to perform out-of-bounds memory reads. For detailed information, refer to CVE-2015-8540.

Note 2462813 provides instructions for securing dynamic selections in SQL queries using the function module FREE_SELECTIONS_RANGE_2_WHERE. The instructions are intended to mitigate SQL injection attacks against the Revenue Accounting application in SAP ERP. Successful SQL injection exploits can lead attackers to perform administrative database operations including reading, modifying and deleting sensitive data.

Note 2433777 deals with authorization errors in the ABAP File Interface used to edit files stored in SAP application servers. The Interface does not effectively perform authority checks for file or path names containing specific control characters. This could enable attackers to access restricted files. As a result, the corrections packaged with the Note disable the ABAP statements



SAP Security Notes by Vulnerability Type

OPEN DATASET and DELETE DATASET for file names with control characters.

Note 2441560 removes a denial of service vulnerability in SAPCAR that could be exploited by attackers to gain root access to servers processing prepared archives. SAPCAR is a utility that is used to compress and decompress files delivered by SAP. SAPCAR 7.21 should be updated to patch level 816 or higher to address the vulnerability.

Appendix: SAP Security Notes, May 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2380277	BC-FES-IGS	Memory Corruption vulnerability in IGS
MEDIUM	2423486	BC-DB-DBI	Missing Authorization check in SAP NetWeaver ADBC Demo Programs
MEDIUM	2236654	CRM-MKT-MPL-CA	XXE Vulnerability in CRM-MKT-MPL-CA
MEDIUM	2374661	BC-WD-UR	Cross-Site Scripting (XSS) vulnerability in Unified Rendering / SAP GUI for HTML
MEDIUM	2316723	BC-FES-ITS	Cross-Site Request Forgery (CSRF) vulnerability in Dynpro Processing in SAP GUI for HTML
MEDIUM	2462813	FI-RA	SQL Injection Vulnerability in Revenue Accounting
MEDIUM	2235515	BC-UPG-NA	Insufficient logging in SNOTE
MEDIUM	2433777	BC-ABA-LA	Missing Authorization check in ABAP File Interface
MEDIUM	1812283	BC-FES-BUS-HTM	Unauthorized modification of displayed content in NWBC
MEDIUM	2394024	IS-DFS-MM-LE	Missing Authorization check in EA-DFPS
MEDIUM	2376743	IS-DFS-BIT-DIS	Missing Authorization check in EA-DFPS utilities
MEDIUM	2448972	BC-FES-JAV	Improved Permission Checks for opening connection in SAP GUI for Java
MEDIUM	2443586	BC-SEC-LGN-SML	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Authentication and SSO
MEDIUM	2442630	IS-DFS-PM	Missing Authorization check in EA-DFPS
MEDIUM	2441560	BC-INS-TLS	Potential Denial of Service (DoS) in SAPCAR

Appendix: SAP Security Notes, May 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2424671	BC-SRV-GBT-GOS	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Generic Object Services
MEDIUM	2412897	EP-PIN-PRT	Cross-Site Scripting (XSS) vulnerability in Enterprise Portal
LOW	2185122	CA-MDG-APP-FIN	Switchable authorization checks for RFC in data extraction within CA-MDG-APP-FIN
LOW	2406918	BC-ESI-WS-JAV-CFG	Missing XML Validation vulnerability in SAP NetWeaver Web Services Configuration UI

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