Layer Seven Security

ADVISORY

SAP Security Notes

June 2016

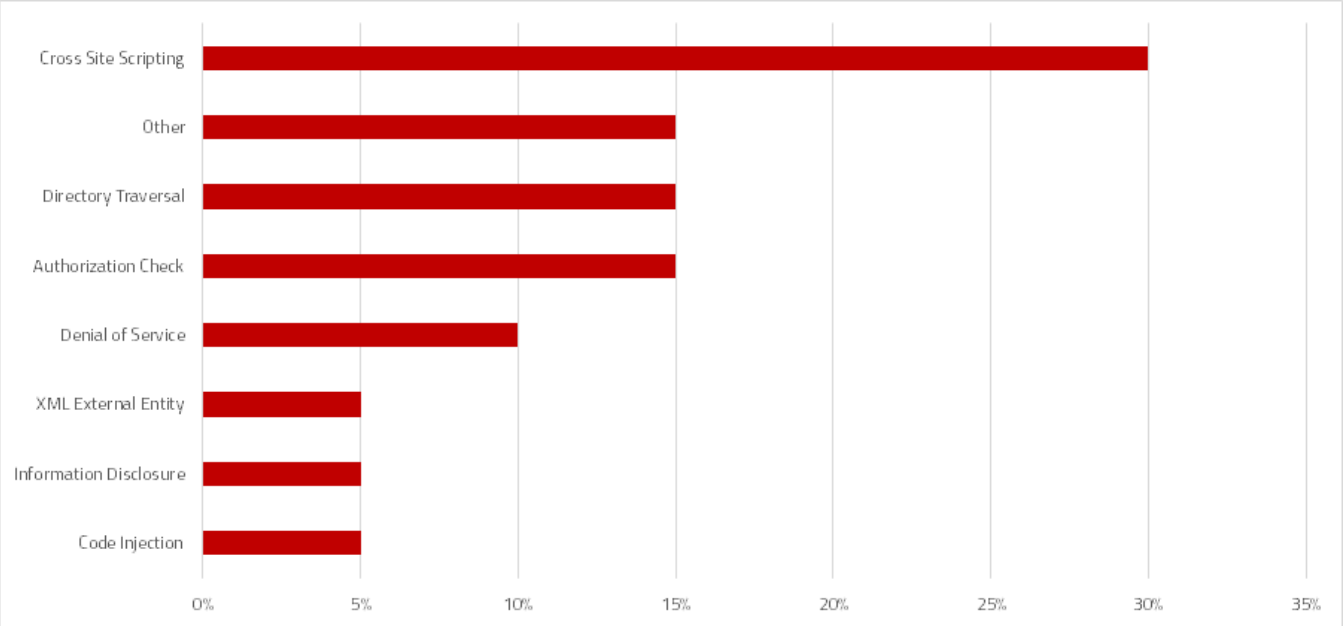
SAP Security Notes

June 2016

Hot News Note 2306709 deals with a code injection vulnerability in Document and Translation Tools (SAPterm). SAPterm manages standard terminology within organizations through transaction STERM. The vulnerability enables attackers to inject malicious code that is subsequently executed by SAPterm. It carries a CVSS rating of 9.1/ 10 and scores low in terms of attack complexity and high for impact. The vulnerability effects releases 731, 740 and 750 of the software component SAP_BASIS. Correction instructions and patches for each release are included in Note 2306709.

SAP released several notes to address cross-site scripting (XSS) and clickjacking vulnerabilities in numerous application areas. Clickjacking occurs when users inadvertently click on malicious hyperlinks embedded in legitimate content. The hyperlinks redirect to pages owned by untrusted applications or domains and can lead users to unknowingly share sensitive information with attackers including username/ password combinations and other forms of authentication data. Notes 2198329, 2011652, 2256178, 2255588, 2254648, and 2246608 include patches for XSS and clickjacking vulnerabilities in components of Business Intelligence, Supply Chain Management, Enterprise Portal and NetWeaver Application Server Java.

Note 2306571 removes a high risk denial-of-service vulnerability in the job server of Data Services by applying input validation for message sequences and closing socket connections for rogue clients.



SAP Security Notes by Vulnerability Type

Note 2293958 recommends using TLS/ SSL for the daemon service in SAP HANA used to start, stop and restart HANA services. TLS/ SSL will encrypt network communications and authenticate clients/ servers to protect the credentials of the OS user configured for the daemon service. This will safeguard against denial of service attacks targeted at the service.

Finally, Note 2252312 changes the severity level of rejected callbacks and callbacks performed in simulation mode logged in the Security Audit Log to Critical. This will ensure that the actions are logged in systems that are configured to log critical events only.

Appendix: SAP Security Notes, June 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2306709	BC-DOC-TER	Code Injection vulnerability in Documentation and Translation Tools
HIGH	2256178	BC-TWB-TST-ECA	Cross-Site Scripting (XSS) vulnerability in ecattping
HIGH	2308217	CA-SUR	Missing XML Validation vulnerability in Web-Survey
HIGH	2306571	EIM-DS	Denial of service (DOS) in SAP Data Services
MEDIUM	2198329	BI-BIP-CMC	Clickjacking issue in CMC- Security Issue
MEDIUM	2255588	BI-RA-AD	Cross-Site Scripting (XSS) vulnerability in SAP BusinessObjects Design Studio
MEDIUM	2254648	EP-KM-TLS-PP	Cross-Site Scripting (XSS) vulnerability in KM People Finder
MEDIUM	2197262	BW-PLA-IP	Information Disclosure in BI Reporting and Planning
MEDIUM	2246608	BC-JAS-SEC-LGN	Cross Site Scripting (XSS) vulnerability in the Logon Application
MEDIUM	2308778	BC-SYB-SQA	Denial of service (DOS) in Sybase SQL Anywhere MobiLink Synchronization Server
MEDIUM	2307494	BC-TRX-API	Missing Authorization check in TREX ABAP+JAVA API
MEDIUM	2303386	BC-BMT-OPI-PVE	Missing authorization check in SAP Operational Process Intelligence
MEDIUM	2293958	HAN-DB	Missing communication security for SAP HANA daemon service
MEDIUM	2316249	SD-MD-CH	Missing Authorization check in SD-MD-CH
MEDIUM	1909843	XX-CSC-PT-FIAA	PT-FIAA: Potential Directory Traversal
MEDIUM	2272676	BC-WD-CMP-ALV-ABA	FPM List UIBB ATS/FPM Tree UIBB/WD ALV: Spreadsheet Formula Injection
MEDIUM	2252312	BC-MID-RFC	Insufficient logging of RFC in SAL
MEDIUM	2297003	EC-PCA-IS	Missing Authorization check in EC-PCA-IS
LOW	2011652	SCM-BAS-UIF	Unauthorized modification of displayed content in SCM-BAS-UIF
LOW	2300346	EIM-DS	Directory Traversal vulnerability in SAP Data Services

LAYER SEVEN SECURITY

Layer Seven Security empowers organisations to realize the potential of SAP systems. We serve customers worldwide to secure systems from cyber threats. We take an integrated approach to build layered controls for defense in depth

Address
Westbury Corporate Centre
Suite 101
2275 Upper Middle Road
Oakville, Ontario
L6H 0C3, Canada

Web
www.layersevensecurity.com
Email
info@layersevensecurity.com
Telephone
1 888 995 0993