ADVISORY

Layer Seven Security

SAP Security Notes

December 2016

Note 1699041 deals with a dangerous directory traversal vulnerability that could enable attackers to read or delete files on SAP servers, leading to the corruption or modification of data. Directory traversal or path traversal vulnerabilities arise from the ability of attackers to access files and directories that are stored outside root folders. This includes directories storing sensitive information such as password hashes or encryption keys.

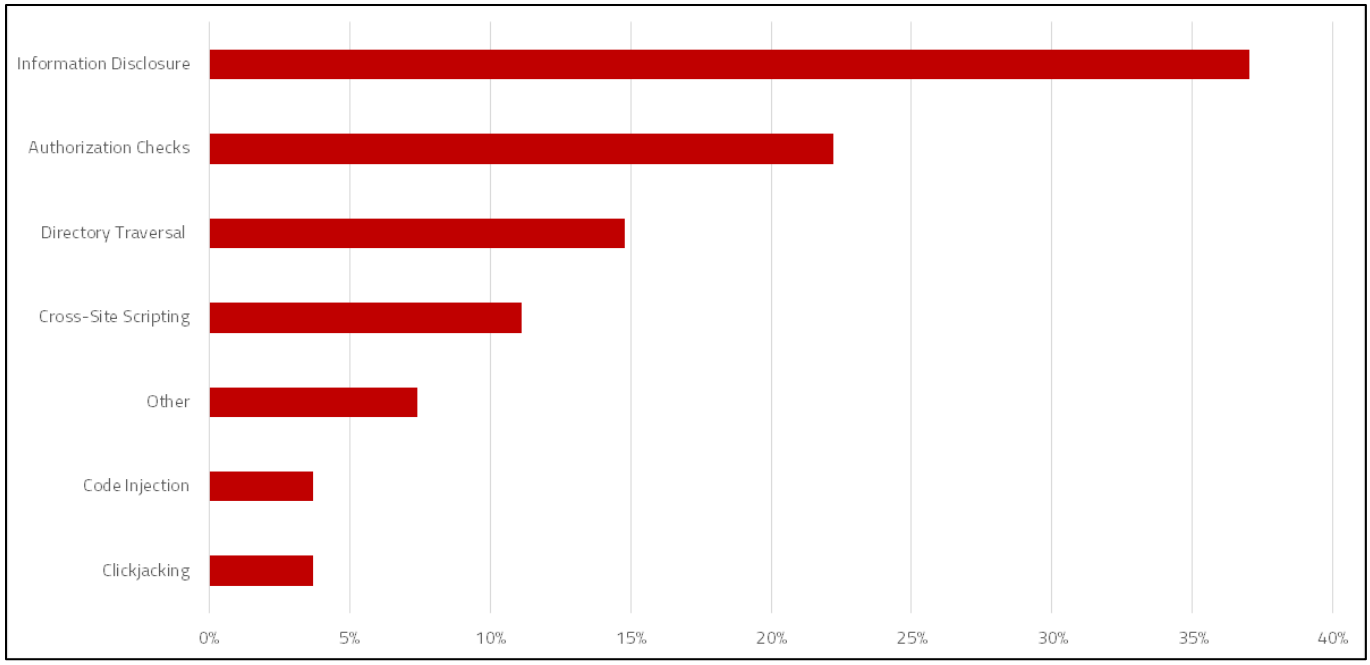
Directory traversal attacks can be mitigated by filtering user inputs, also known as input validation. This includes normalizing characters and removing meta characters. Also, logical file names should be defined to validate physical file names.

Note 1699041 provides logical path names for the vulnerable software component XX-CSC-BR-REP in SAP_APPL. The latter is a core ECC application area for Logistics and Accounting. The corrections are delivered through the relevant support packages for SAP_APPL versions 46C – 606. The Note has multiple dependencies including the prerequisite Note 1497003.

Note 2394445 removes an information disclosure vulnerability in SAP HANA that could enable attackers to extract details of available users in HANA through the user self-service application. The exploit can be performed remotely and without authentication. User self-service tools are disabled by default and are maintained through parameters in the xsengine.ini file.

SAP Security Notes

December 2016



SAP Security Notes by Vulnerability Type

Note 2351486 deals with a similar information disclosure vulnerability in the HANA Cockpit that could allow attackers to read files from the server file system with the credentials of the <sid>adm operating system user.

Other information disclosure vulnerabilities are addressed by Notes such as 2336393, 2344524 and 2283666 in platforms that include Business Objects, Business Intelligence and the NetWeaver Application Server.

Note 2336795 removes a flaw in functionality within Business Objects (BOBJ) that could be abused to perform port scans for systems in the internal network connected to BOBJ. This could lead to the disclosure of available services and installed operating systems to further attacks against SAP servers.

Appendix: SAP Security Notes, December 2016 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	1699041	XX-CSC-BR-REP	IN86: Potential Directory Traversal
HIGH	2336393	BI-RA-WBI-BE-SM	Information Disclosure in Business Objects Explorer
HIGH	2265964	BI-BIP-INV	Deserialization of untrusted data in BI Platform
MEDIUM	2265385	CRM-ISA-CAT	Switchable authorization checks for RFC in Product Catalog
MEDIUM	2344524	BC-GP	Information Disclosure in Guided Procedures
MEDIUM	2373032	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in WebClient User Interface
MEDIUM	2394445	HAN-AS-XS-ADM	Information disclosure in SAP HANA XS classic user self service
MEDIUM	2250817	BI-BIP-INV	Cross-Site Scripting (XSS) vulnerability in Infoview - Titan
MEDIUM	2310790	BC-JAS-SEC-UME	Directory Traversal Vulnerability in a UserAdmin Application
MEDIUM	2351486	HAN-CPT	Information disclosure in SAP HANA cockpit for offline administration
MEDIUM	2359019	BC-SYB-SQA	'FalseConnect' HTTP Proxy Authentication vunerability with MobilLink clients and Relay Server Outbound Enabler
MEDIUM	2376998	IS-DFS-BIT-DIS	Missing Authorization check in EA-DFPS monitoring tools
MEDIUM	2336795	BI-RA-CR	Port scanning via URL Reporting in SAP BusinessObjects Enterprise
MEDIUM	2375140	BC-GP	Update 1 to Security Note 2344524
MEDIUM	2374749	IS-DFS-MA	Missing Authorization check in SAP Mobile Defense & Security 1.6
MEDIUM	2374165	BW-PLA-BPS	Missing Authorization check in BW Business Planning and Simulation
MEDIUM	2373175	BC-MID-ICF-LGN	Information Disclosure in ABAP HTTP system logon page
MEDIUM	2283666	BI-BIP-INV	Potential information disclosure in Business Objects Explorer
MEDIUM	2377067	IS-DFS-BIT-DIS	Missing Authorization check in EA-DFPS synchronization mechanisms
MEDIUM	2378065	SBO-CRO-SEC	Missing XML Validation Vulnerability in SAP Business One

Appendix: SAP Security Notes, December 2016 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2360488	EP-PIN-NAV-FFP	Cross-Site Scripting (XSS) vulnerability in Fiori Launch Pad on Enterprise Portal
MEDIUM	2288991	BI-BIP-ADM	Directory Traversal vulnerability in SAP BusinessObjects Platform
LOW	2179233	LO-MD-BP-CM	Missing authorization check in LO-MD-BP-CM, LO-MD-BP-VM, FI-AP-AP-N, FI-AR-AR-N
LOW	2379342	HAN-DB-BAC	Cross-Site Scripting (XSS) vulnerability in backup function of SAP HANA cockpit
LOW	2368082	BC-DWB-UTL	Information Disclosure in ABAP Development Environment
LOW	2354254	BI-RA-AWB	Information Disclosure in SAP Business Intelligence Analysis for OLAP
LOW	2244161	WEC-FRW	Clickjacking Protection in Web Channel Experience Management (WCEM)

LAYER SEVEN SECURITY

Layer Seven Security empowers organizations 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
555 Industrial Drive
Suite 107
Milton, Ontario
L9T 5E1, Canada

Web
www.layersevensecurity.com
Email
info@layersevensecurity.com
Telephone
1-647-964-7370

Layer Seven Security offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Layer Seven Security makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.