Layer Seven Security

ADVISORY

SAP Security Notes

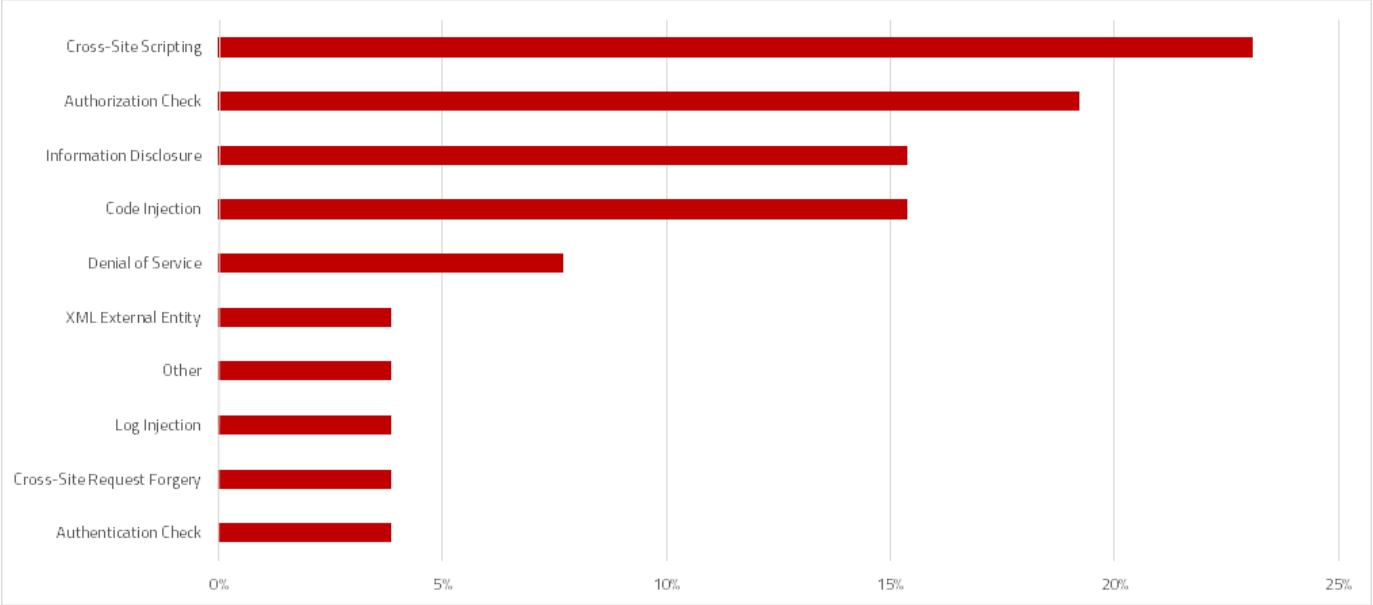
January 2016

SAP Security Notes

January 2016

SAP released several high priority Notes in January for the Java deserialization vulnerability in Apache libraries found in the Enterprise Portal, Process Integration and Sybase products including the ASE relational database. The Java deserialization vulnerability impacts applications that accept serialized Java objects from untrusted sources. The proof of concept for the vulnerability was released in early 2015. However, most software vendors effected by the flaw did not respond until November following the release of a research paper that demonstrated a working exploit for the vulnerability. The Java deserialization vulnerability can be exploited to inject malicious code into bytes that are reassembled into objects during the deserialization process if the code is not validated before it is executed. The impact can be catastrophic and can include the complete compromise of servers executing the code. Customers are strongly advised to apply the patches for the EP runtime, PI gateway applications, and other components included in Notes 2249347, 2247644, and 2262645.

Note 2246277 recommends setting the REMOTE_OS_AUTHENT parameter in Oracle 11.2 databases to false. This will prevent attackers from connecting to the database without supplying a password by impersonating users that are authenticated by the operating system. The SQL commands for checking and changing the value of the parameter are provided in the Note. REMOTE_OS_AUTHENT has been deprecated in Oracle 12.1 due to the significant risks associated with OS authentication for database access.



SAP Security Notes by Vulnerability Type

Note 2251619 introduces an authority check for the authorization object S_RZL_ADM in the function module DB6_ADM_WRITE_AUDIT_LOG. This is intended to secure access to the audit log of the DBA Cockpit used to monitor and administer databases. The log tracks changes made to database objects from the Cockpit including details of specific SQL commands, source and target systems, and users.

Note 2241978 addresses a similar risk associated with debug functions within earlier versions of SAP HANA Extended Application Services (XS) that can be exploited by attackers to update trace files without authentication. Customers should implement the support package referenced in the Note or block access to URLs for the HANA debugger using network firewalls, reverse proxies or the Web Dispatcher.

Appendix: SAP Security Notes, January 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2251619	BC-DB-DB6-CCM	Missing authorization check in Audit Functions of DBA Cockpit
HIGH	2249347	EP-PIN-PRT	Security vulnerabilities found in Apache Commons Collections library used in ep.runtime.common
HIGH	2247644	BC-XI-IGW	PI SEC: Security vulnerabilities found in Apache Groovy Library used in PI Cloud Integration Content
HIGH	2206793	BC-NWA-XPI	Unauthorized modification of displayed content in RWB
HIGH	2191290	BC-JAS-SEC-UME	Potential information disclosure relating to AS Java
HIGH	2262645	BC-SYB-ASE	Security vulnerability in Apache Commons Collections library used by multiple SAP Sybase products.
HIGH	2246277	BC-DB-ORA-INS	SAP ORACLE insecure authentication scheme
HIGH	2167813	BC-XI-IBD	Potential information disclosure relating to Enterprise Services Repository
HIGH	2243373	BC-WD-JAV	Potential denial of service in BC-WD-JAV
HIGH	2239015	MOB-UIA-LIB-AUT	Unauthorized modification of displayed content in Fiori Login class
HIGH	2234918	BC-SRV-PMI	Unauthorized modification of displayed content in PMI
HIGH	2227310	EP-PIN-TOL	Unauthorized modification of displayed content in com.sap.portal.themes.integrity
HIGH	2224249	EP-PIN-DNT	Unauthorized modification of stored content in ConfigEditor
MEDIUM	1865646	FIN-SEM-CPM-BSC	Unauthorized modification of displayed content in FIN-SEM-CP
MEDIUM	2214442	LO-VC-LOI	Missing authorization check in SCM-APO-INT-MD-PDS
MEDIUM	2244346	CRM-ISA	Untrusted XML input parsing possible in CRM-ISA
MEDIUM	2257327	IS-U-EIM	Missing authorization check in IS-U-EIM
MEDIUM	2252941	HAN-DB	Potential information disclosure relating to files exported from SAP HANA with EXPORT statement
MEDIUM	2248735	BC-ABA	Code injection vulnerability in System Administration Assistant
MEDIUM	2193424	EP-PIN-NAV-AFP	Potential information disclosure relating to NavigationServlet
MEDIUM	2241978	HAN-AS-XS	Log injection and missing size restriction in SAP HANA Extended Application Services Classic (XS)
MEDIUM	2233550	HAN-DB	Communication encryption for HANA multi tenant database containers does not work as expected
MEDIUM	2233136	HAN-DB	Potential termination of running processes triggered by IMPORT statement
MEDIUM	2221986	HAN-AS-RUL	Too many privileges assigned to HANA hdbrole
MEDIUM	1973081	BC-ABA-SC	XSRF vulnerability: External start of transactions with OKCode
LOW	2180125	LE-TRM	Missing authorization check in LE-TRM

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