Layer Seven Security

ADVISORY

SAP Security Notes

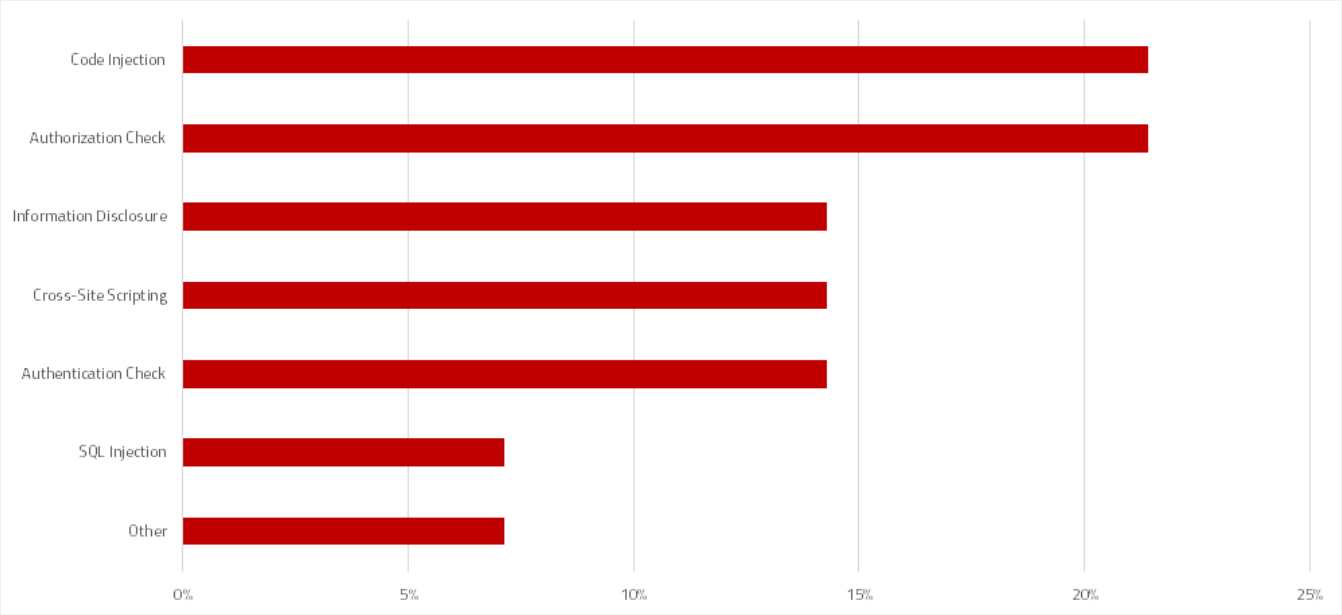
May 2016

SAP Security Notes

May 2016

SAP issued a Hot News note for a dangerous missing authentication check in the ASE XP Server. The XP Server typically runs on the same host as ASE. It is used to execute extended stored procedures (ESP) through remote procedure calls (RPC). XP Server is automatically installed with ASE and is required by ASE to execute an ESP. The missing authentication check addressed by Note 2296023 could enable attackers to read, modify or delete sensitive information and perform other privileged functions. The Note carries a CVSS score of 9/10 and rates high on impact. The related attack vector also has a high exploit range and does not require any credentials for successful execution. The vulnerability impacts ASE versions 15.7 and 16.0. Customers should implement the releases listed in the Solution section of Note 2296023.

Note 2307384 provides a patch for the Java deserialization vulnerability in the Business Objects solution SAP Predictive Analytics which is used for statistical analysis and data mining. Similar to other solutions patched by SAP in earlier months for the identical vulnerability, Predictive Analytics uses the Apache Commons Collection. This is a framework within the Java Development Kit (JDK) that is vulnerable to a remote code execution attack caused by the failure to validate java objects from untrusted sources. The issue impacts earlier versions of Predictive Analytics and can be fixed by upgrading to versions 2.5 or later. The system property org.apache.commons.collections.enableUnsafeSerialization is set to true in later versions and deserialization support for unsafe classes in the functor package is removed.



SAP Security Notes by Vulnerability Type

Note 2298367 provides corrections for the deserialization vulnerability in Crystal Reports for Enterprise.

Other important Security Notes include 2317756, 2222731 and 2281002. The Notes address vulnerabilities for code injection in CRM Fiori apps, cross-site scripting in BI Design Studio, and information disclosure in the Enterprise Portal, respectively.

Appendix: SAP Security Notes, May 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2296023	BC-SYB-ASE	Missing Authentication check in SAP ASE XPServer
HIGH	2307384	BI-RA-PA	Deserialization of untrusted data in SAP Predictive Analytics
HIGH	2298367	BI-RA-CRE	Deserialization of untrusted data in Crystal Report for Enterprise
MEDIUM	2222731	BI-RA-AD	Unauthorized modification of stored content in DesignStudio SFIN use case
MEDIUM	2317756	CRM-FIO-BTX-TAS	Input length validation missing in CRM Fiori apps
MEDIUM	2160790	FS-CML	Fehlende BerechtigungsprÃ¼fung in FS-CML
MEDIUM	2260876	BC-INS-CTC	Multiple vulnerabilities in LM Configuration Wizard
MEDIUM	2254425	BC-FES-IGS	Clickjacking vulnerability in SAP Internet Graphics Server
MEDIUM	2281002	EP-PIN-CS	Information Disclosure in Portal Netweaver Client Services
MEDIUM	2298657	IS-B-BCA-AM	Missing Authorization check in SAP R/3 Enterprise Financial Services
MEDIUM	2297853	BC-SYB-ASE	Missing Authorization check in SAP ASE
MEDIUM	2296722	BC-SYB-ASE	Information Disclosure vulnerability in SAP ASE Installer
MEDIUM	2195409	LO-SLC	Potential modif./disclosure of persisted data in SAP CPQ Solution Configuration (SME)
LOW	2292487	BC-I18	Hard Coded System IDs in Code Page Conversion Tool (BC-I18)

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