Layer Seven Security

ADVISORY

SAP Security Notes

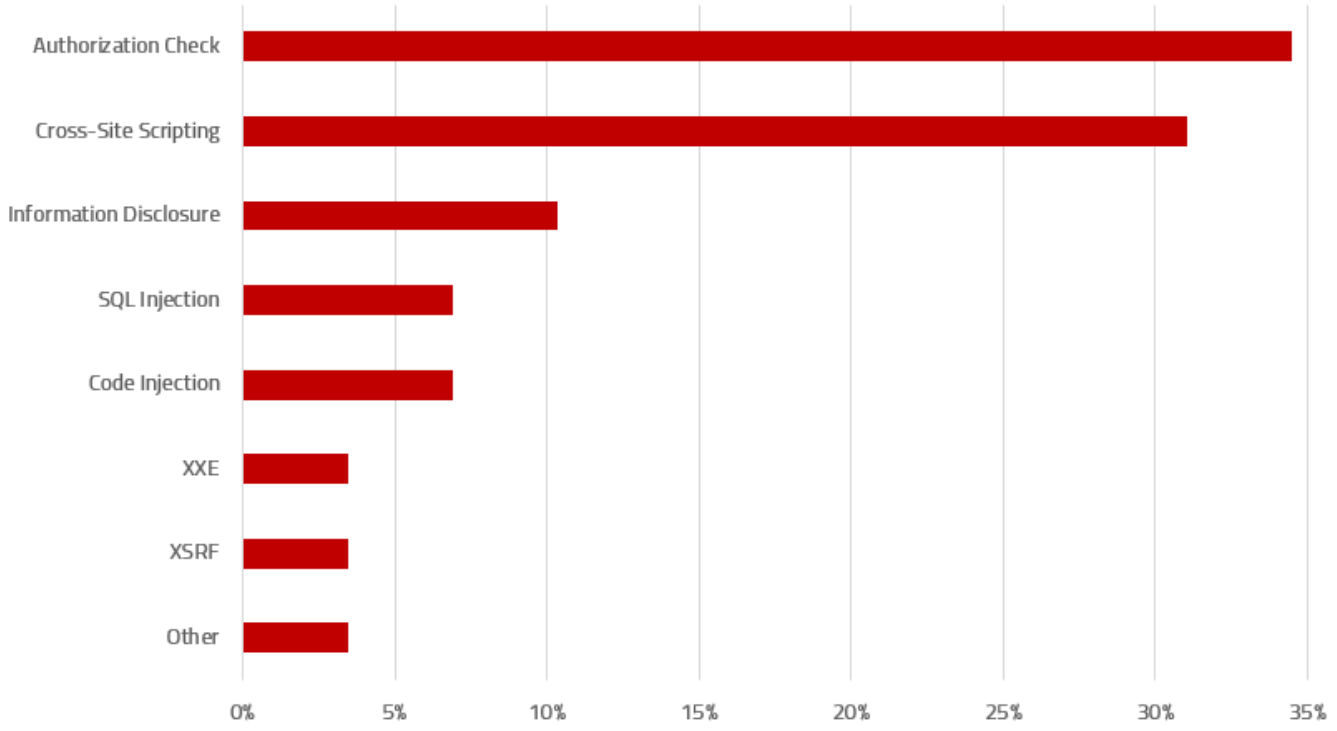
September 2015

SAP Security Notes

September 2015

SAP released a Hot News patch in September for a high-risk remote code execution vulnerability in HANA Extended Application Services (XS). HANA XS is a lightweight application server and development environment embedded within the HANA appliance. It provides access to the HANA database via HTTP-based services such as OData. Note 2197397 addresses a buffer overflow vulnerability in HANA XS that could enable attackers to inject malicious code into working memory that may be subsequently executed by the application. This could allow attackers to take complete control of HANA to access or modify data or provoke a denial of service. The Note includes corrections for SPS08 and SPS09. SPS10 is not effected. In addition to applying the corrections, customers should restrict access to the HANA XS network ports. Access to the relevant ports is a dependency for the exploitation of the vulnerability. The standard ports are 80xx for HTTP and 43xx for HTTPS.

SAP released an unusually high number of Notes for reflected cross-site scripting (XSS) vulnerabilities in September impacting several software components. Reflected or non-persistent XSS attacks differ from stored or persistent XSS attacks in terms of the methods used by attackers to deliver malicious scripts that are executed by client browsers. Unlike persistent attacks, scripts are not stored in application servers but delivered through other routes such as servers or sites controlled by attackers. Notes 2193416, 2161571, 2164648, 2166779, 1929564, 2176785 and 1895848 patch reflected XSS vulnerabilities in areas such as Web Dynpro ABAP and Java, BI Performance Management and LaunchPad, and Java Monitoring.



SAP Security Notes by Vulnerability Type

There were also several high priority Notes released by SAP for missing authorization checks in components of ERP Sales and Distribution. Notes 2155614, 2184117, 2185233 and 2200806 address authorization issues that may lead to an escalation of privileges. The impacted components include Sales (SD-SLD), Customer-Material Information (SD-MD-AM-CMI), Revenue Recognition (SD-BIL-RR) and Foreign Trade (SD-FT).

Finally, Note 2201710 provides an updated product version matrix for Sybase solutions impacted by the Logjam vulnerability that use the Diffie-Hellman key exchange cryptographic algorithm for sharing encryption keys and negotiating secure connections. Logjam vulnerabilities can be exploited by attackers to downgrade TLS connections to insecure 512-bit grades. The OpenSSL cryptographic library used by the impacted Sybase products has been updated to reject handshakes shorter than 768 bits.

Appendix: SAP Security Notes, September 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2197397	HAN-AS-XS	Potential remote code execution in SAP HANA Extended Application Services (XS)
HIGH	2037304	SV-SMG-SDD	Lacks proper input validation in SDCC Download Function Module
HIGH	2155614	SD-SLS	Missing authorization check in SD-SLS, SD-CAS and SD-MD-AM-CMI
HIGH	1677810	IS-U-WA	Unauthorized modification in ITS-Service in IS-U-WA
HIGH	2184117	SD-FT-PRO	Missing authorization check in Foreign Trade
HIGH	2185233	SD-BIL-RR	Missing authorization check in Revenue Recognition
HIGH	2192350	TM-MD-TN-SCH	Missing authorization check in Transportation Management
HIGH	2192554	FIN-FSCM-TRM-TM	Missing authorization check in Treasury
HIGH	2193416	BC-WD-JAV	Unauthorized modification of displayed content in WebDynpro Java
HIGH	2200806	SD-FT-PRO	Missing authorization check in Foreign Trade
HIGH	2161571	BI-BIP-INV	Unauthorized use of application functions in BI Workspace
HIGH	2164648	BI-BIP-INV	Unauthorized modification of displayed content in BI LaunchPad
HIGH	2166779	BI-BIP-INV	Unauthorized modification of displayed content in Performance Management Application
HIGH	1929564	BC-WD-ABA	Unauthorized modification of displayed content in BC-WD-ABA
HIGH	2176785	BC-JAS-ADM-MON	Unauthorized modification of displayed content in Java Monitoring
HIGH	1895848	BC-WD-UR	Unauthorized modification of displayed content in UR
HIGH	2180655	SD-MD-CM	Missing authorization check in Condition Maintenance
HIGH	2183189	BC-FES-BUS-RUN	Untrusted XML input parsing possible in the runtime of SAP NetWeaver Business Client
HIGH	1507735	IS-M	Unauthorized use of application functions in IS-Media
MEDIUM	1748129	AP-MD-BP	Potential modification of persisted data in AP MD BP
MEDIUM	2053788	BC-MOB-MI-SER	Missing authorization check in RFC enabled function module - BC-MOB-MI-SER
MEDIUM	1861040	CRM-IPS-ICM-REL	Potential disclosure of persisted data in CRM-IPS-ICM-REL
MEDIUM	2191529	BC-TRX-API	Potential information disclosure relating to Transaction SCI (Code Inspector)
MEDIUM	2199045	BC-SRV-KPR-DMF	Unauthorized modification of displayed content in BC-SRV-KPR
MEDIUM	2201710	BC-SYB-PB	Fixing Logjam and Alternative chains certificate forgery vulnerabilities in multiple SAP Sybase products
MEDIUM	2180555	BI-BIP-SL-ENG-REL	Potential information disclosure relating to BusinessObjects Semantic Layer SDK
MEDIUM	1835366	AP-MD-BP	Potential disclosure of persisted data in AP MD BP
MEDIUM	2165838	FIN-FSCM-TRM-TM-TR	Missing authorization check in Transaction Management
LOW	2197174	BC-SEC-SSF	Missing authorization check in SAP Kernel

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