Layer Seven Security

ADVISORY

SAP Security Notes

April 2016

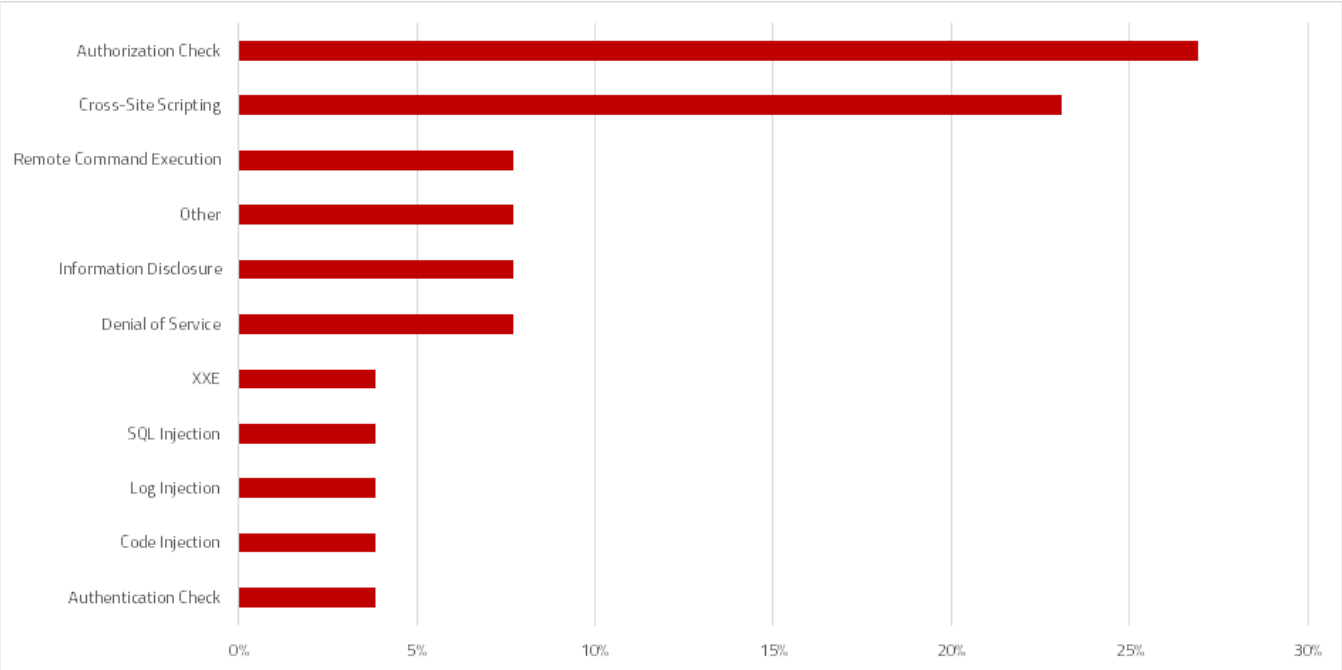
SAP Security Notes

April 2016

SAP released a series of Notes in April for vulnerabilities identified in the SAP HANA Data Provisioning (DP) Agent. The DP Agent is a component of Smart Data Integration (SDI) used to acquire, replicate and transform data from external sources in releases SPS09 or higher of the HANA platform. This includes data from Cloud, on-premise and Web sources. Typically, DP Agents are installed on source systems, rather than directly in HANA systems. This is both for performance and security reasons.

The Agents use a TCP or HTTP connection to communicate with HANA systems. The default communication channel is insecure and should be secured using HTTPS after installation through the DP Agent Configuration Tool. The local port 5051 is used for internal communication between the DP Agent and the Configuration Tool. Remote access to the port should be blocked to prevent unauthorized changes in DP agents.

Note 2262742 recommends taking this a step further by binding connection requests to port 5051 to localhost. This will only allow connections from within the same host. Note 2280054 recommends enabling SSL to secure the communication link with DP Agents. This will protect against data leaks impacting sensitive information transmitted through the channel. Finally, Note 2262710 includes a fix to validate the length of packets transmitted to DP Agents to secure against attacks that generate a denial of service using requests that provoke resource exhaustion.



SAP Security Notes by Vulnerability Type

Note 2258784 deals with a similar high priority vulnerability in the standalone enqueue server. A denial of service impacting the enqueue server could interrupt client application servers in distributed, high-availability environments. The Note provides a kernel patch that updates the internal variables of the enqueue server initialized at start time.

Notes 2252191 and 2265514 deliver corrections for the Java deserialization vulnerability in HANA XS and the Mobile Platform. In earlier months, SAP released fixes for the bug in EP, PI and ASE. The Java deserialization vulnerability is a dangerous code injection flaw that impacts open source Apache libraries installed in many Java components found in SAP systems. Details of the vulnerability are published in CVE-2015-3253 available at the National Vulnerability Database.

Lastly, Note 2254389 contends with XML External Entity (XXE) attacks that could be exploited to perform a denial of service in the SAP UDDI Server. The server is a component of AS Java that contains the registry of available Web services in SAP systems including information such as consumers, systems and relevant metadata. The Note references relevant Support Packages that patch the XML parser in AS Java to block external entities in incoming XML documents.

Appendix: SAP Security Notes, April 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2262742	HAN-DP-SDI	Missing Authentication check in HANA DP Agent
HIGH	2252191	BC-XS-JAS	Deserialization of untrusted data in SAP HANA XS Advanced Java Runtime
HIGH	2254389	BC-ESI-UDDI	XXE vulnerability in SAP UDDI
HIGH	2262710	HAN-DP-SDI	Denial of service (DOS) vulnerability in HANA DP Agent
HIGH	2258784	BC-CST-EQ	Denial of service (DOS) vulnerability in Enqueue Server
HIGH	2265514	OPU-GW-JAV	Deserialization of untrusted data in Groovy Engine
HIGH	2294689	BC-SYB-ASE	SQL Injection vulnerability in SAP ASE
MEDIUM	1444282	BC-CST-GW	gw/reg_no_conn_info settings
MEDIUM	1850010	CRM-CM	Potential modif./disclosure of persisted data in CRM-CM
MEDIUM	1933375	XX-CSC-RU-FI	RU ERP for Banking. Missing authorization check. Potentential modification of persisted data
MEDIUM	2043447	SV-SMG-TWB-BCA	Missing authorization check in SV-SMG-BPCA
MEDIUM	2051717	BC-CCM-MON-ORA	[MUNICH] Review of Testcase 100
MEDIUM	2201916	XX-CSC-IN-FI	Missing authorization check in XX-CSC-IN-FI
MEDIUM	2289575	CRM-CCI	Cross-Site Scripting (XSS) vulnerability in SAP Contact Center Infrastructure when handling chats, e-mails, call extra data, scripts, and presence and directory data
MEDIUM	2300197	SV-SMG-SUP	Cross-Site Scripting (XSS) vulnerability in SAP Solution Manager Fiori Apps 'My Incidents' and 'My Business Requirements'
MEDIUM	2280054	HAN-DP-SDI	Information Disclosure in Data Provisioning Agent
MEDIUM	2201295	BC-WD-UR	Cross-Site Scripting (XSS) vulnerability in UR Control.
MEDIUM	2274560	BC-CST-GW	Arbitrary Log File Injection vulnerability in SAP Gateway
MEDIUM	2274286	BI-BIP-INV	Cross-Site Scripting (XSS) vulnerability in BI Documents send action.
MEDIUM	2273241	CRM-ISA-TEC	Cross-Site Scripting (XSS) vulnerability in Internet Sales
MEDIUM	2267789	BC-MUS-LP	Missing authorization checks in Report Launchpad component
MEDIUM	2263719	BC-WD-JAV	Cross-Site Scripting (XSS) vulnerability in BC-WD-JAV
MEDIUM	2221657	BC-CST-IC	Code injection vulnerability in SAP Internet Communication Manager
MEDIUM	2297003	EC-PCA-IS	Missing Authorization check in EC-PCA-IS
MEDIUM	2284952	BC-CUS-TOL-HMT	Update 2 to Security Note 1971238
MEDIUM	1951340	XX-CSC-HU-FI	Missing authorization check in XX-CSC-HU-FI

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