Layer Seven Security

ADVISORY

SAP Security Notes

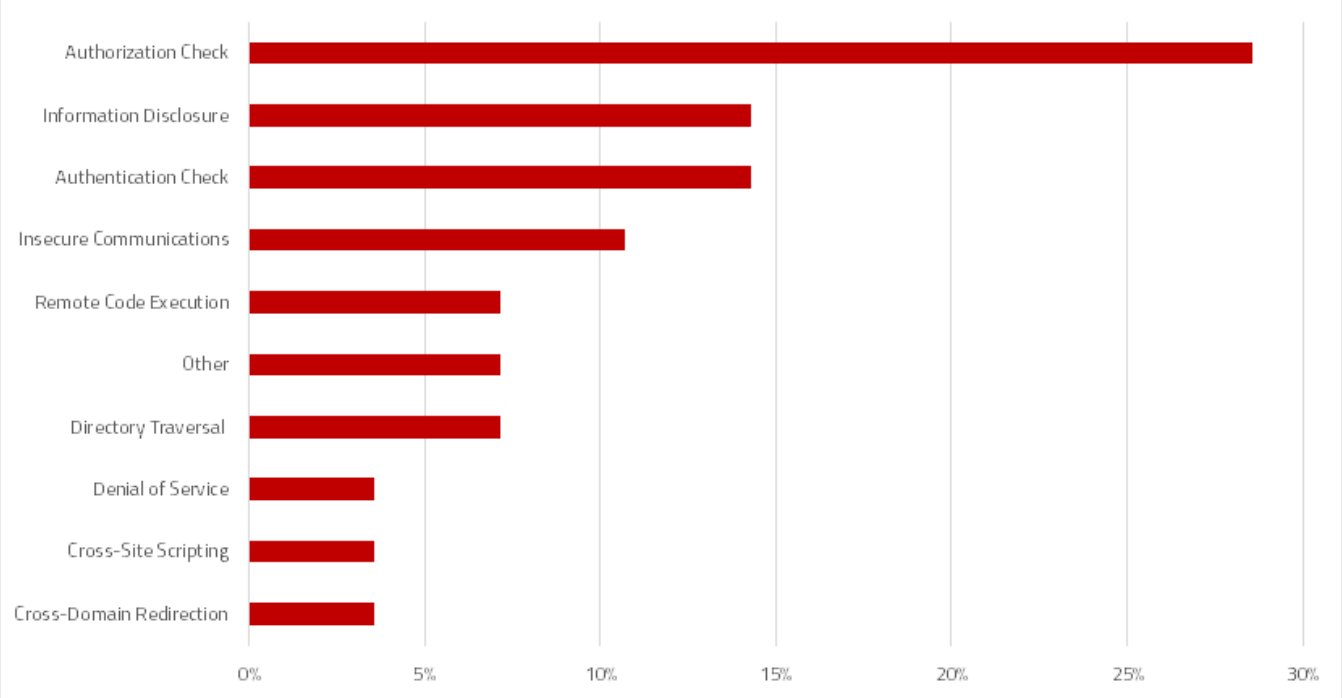
October 2015

SAP Security Notes

October 2015

SAP released a batch of emergency fixes for the Download Manager (SDM) application through Notes 2235412 and 2233617 in October. The Notes appeared to have been hastily released in response to an event that SAP described as an 'irresponsible disclosure' by a security researcher. In other words, the researcher did not follow standard disclosure practices that forewarn the SAP Product Security Response Team for newly discovered security vulnerabilities and provide sufficient time to develop, test and release appropriate security fixes before public disclosures. SDM is used to transfer installation and other files from the SAP Support Portal. Customers are strongly advised to implement version number 2.1.142 of SDM to remove a dangerous flaw that exposes the application to man-in-the-middle, directory traversal and other attacks.

There were also several important Notes released for serious vulnerabilities impacting SAP HANA. Given the strategic importance of HANA for SAP, many of these vulnerabilities received a great deal of press attention. The most critical vulnerability was a remote code execution flaw addressed by Note 2197428. Customers should limit network access to the SQL and XS ports to prevent connections from unknown sources. Notes 2197459 and 2216869 deal with vulnerabilities that could impact the integrity of HANA logs and allow brute-force attacks against the SYSTEM user. Patches are bundled in the relevant Support Packages referenced in the Notes. The patches include two new parameters to support password locks for the SYSTEM user and prevent the disclosure of detailed information for failed logon attempts



SAP Security Notes by Vulnerability Type

Note 2203591 provides recommendations for securing the RFC connection between TREX or BWA installations and BW systems. This connection could be abused to execute OS commands on TRX/ BWA hosts. The solution requires maintaining entries in the access control list of the reginfo file on the TRX/BWA host. This will restrict communication for the registered program of the TRX/ BWA host to internal and local scenarios only.

Finally, 2149706 removes an information disclosure in the System Landscape Directory (SLD) of Java Application Servers. The vulnerability could be exploited to disclose host names and SAP System IDs (SIDs) through the user interface of the SLD. This information is often required to perform targeted attacks against SAP systems.

Appendix: SAP Security Notes, October 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2235412	XX-SER-SAPSMP-SDM	Security Vulnerabilities in SAP Download Manager
HOT NEWS	2233617	XX-SER-SAPSMP-SDM	Security Vulnerabilities in SAP Download Manager
HOT NEWS	2197428	HAN-DB	Potential remote code execution in HANA
HIGH	2179615	CA-VE-VEV	Potential remote code execution in SAP 3D Visual Enterprise Author, Generator and Viewer
HIGH	2194730	BC-SRV-MCM	Multiple vulnerabilities in SAP Mobile Document Android Client
HIGH	2195595	BC-BSP	Multiple security vulnerabilities in SAP NetWeaver BSP Logon
HIGH	2197459	HAN-DB	Potential log injection vulnerability in SAP HANA audit log
HIGH	2203591	BC-TRX	TREX/BWA installation can be attacked via RFC-Gateway
HIGH	1983443	FI-AP-AP-B1	Missing authorization check in FI-AP-AP-B1
HIGH	2149706	BC-CCM-SLD	Potential information disclosure relating to NW AS Java
HIGH	2159481	SD-SLS-GF	Missing authorization check in Sales Order Monitor (VA06)
HIGH	2219924	FI-AP-AP-B1	Missing authorization check in FI-AP-AP-B1
HIGH	2216869	HAN-DB-SEC	Security improvement of HANA authentication
HIGH	2215605	FI-AP-AP-B1	Missing authorization check in FI-AP-AP-B1
MEDIUM	1937165	FI-BL-PT-US	Directory traversal in FI-BL-PT-US / FI-BL-PT-PR
MEDIUM	2053788	BC-MOB-MI-SER	Missing authorization check in RFC enabled function module - BC-MOB-MI-SER
MEDIUM	2193214	BC-MID-ICF	Potential false redirection of Web site content in SAP Internet Communication Framework
MEDIUM	2189853	BC-MID-ICF	SAP Internet Communication Framework fails to validate HTTP_WHITELIST
MEDIUM	1957910	BC-CCM-FIL	Directory traversal in BC-CCM-FIL
MEDIUM	2103389	BC-VMC	Missing authorization check in BC-VMC
MEDIUM	2164133	BC-FES-IGS	Potential remote termination and denial of service in IGS
MEDIUM	2226028	MOB-SDK-SEC	Potential information disclosure relating to iOS mobile applications
MEDIUM	2223028	FI-GL-GL-G	Missing authorization check in FI-GL-GL-G
MEDIUM	2170806	MOB-SDK-ODP	DataVault password retry count resets incorrectly
MEDIUM	2074276	XX-SER-SAPSMP-SDM	Potential information disclosure relating to user logon data that is used in SAP Download Manager
MEDIUM	2193389	BC-CCM-BTC	Potential modif./disclosure of persisted data in SAP Batch Processing
MEDIUM	2029397	CRM-ISA-R3	Missing authorization checks for RFC in E-commerce ERP applications
MEDIUM	2061129	FIN-FSCM-DM	Missing whitelist check in SAP Dispute Management

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