Layer Seven Security

ADVISORY

SAP Security Notes

August 2015

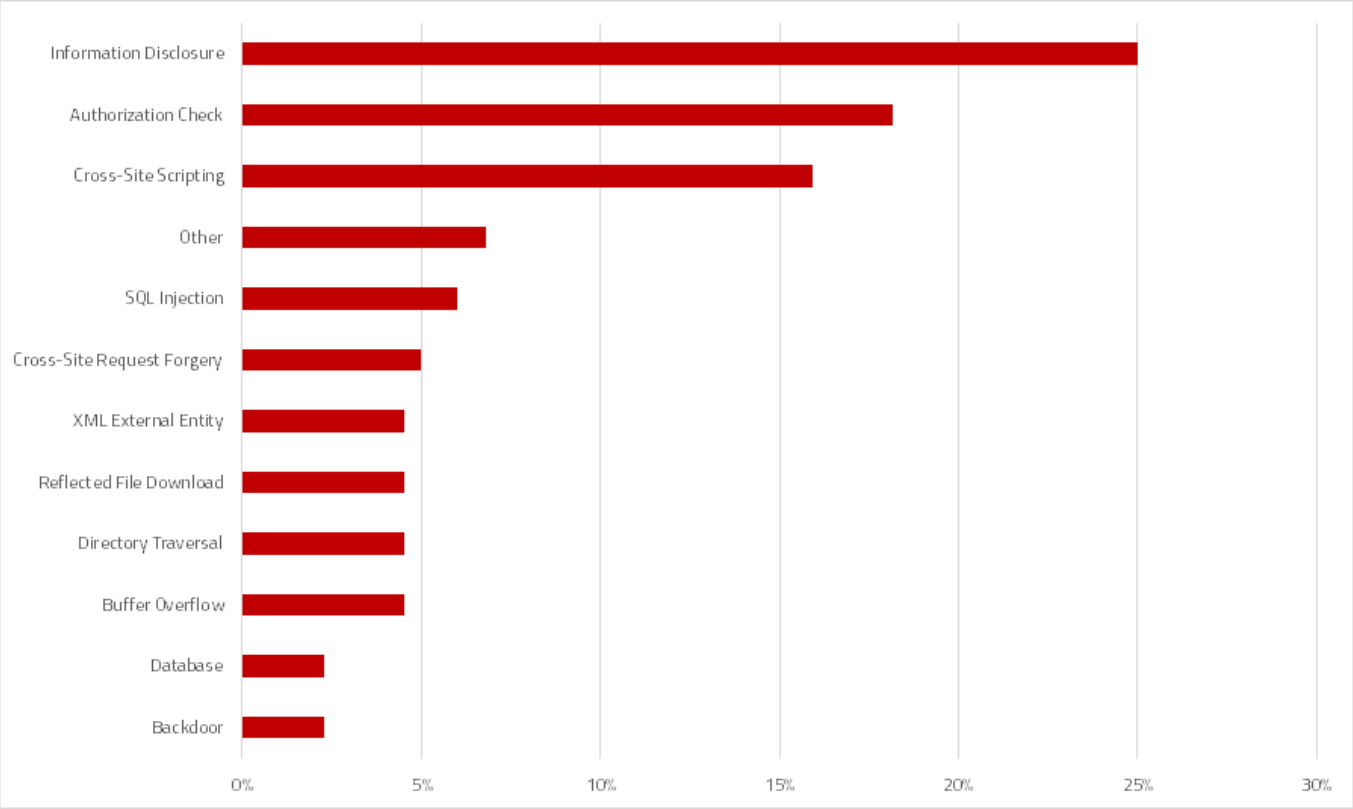
SAP Security Notes

August 2015

One in four of the Security Notes released in August addressed information disclosure vulnerabilities in several SAP products that could lead to the leakage of encryption keys, passwords and other sensitive data. The most critical included Notes 2183624, 2165583, 2180403 and 2157458 impacting HANA, the ABAP Debugger and the Internet Communication Framework. There were also lower priority Notes for components such as the Web Dispatcher (Note 2148905). The Notes emphasize the importance of updating cryptographic libraries, securing trace files, changing default SSFS master keys, and protecting all communications with SSL/ TLS, not just external paths. The importance of these measures should not be underestimated. The impact of some of the most well-publicized data breaches in 2015 so far could have been lessened by the proper application of database and transport layer encryption.

SAP updated Note 850306 for the third Oracle SPU/ PSU of the year. This Note should be periodically checked by customers with SAP installations containing Oracle databases. Oracle Security Patch Updates (SPU) and Patch Set Updates (PSU) are packaged into SAP Bundle Patches (SBP). SBPs for Oracle are released every four months and are targeted at critical and severe database issues including security vulnerabilities.

Note 1562697 contains instructions for creating an authorization group for table RFCSYSACL. This table is generally assigned to the standard SC authorization group. SAP recommends creating a dedicated group called TTRL to restrict the ability to view trust relationships configured between SAP systems. This can be



SAP Security Notes by Vulnerability Type

performed using the general table maintenance transaction SE54.

Note 2182768 modifies the APIs HTTP_ACTIVATE_NODE and HTTP_INACTIVATE_NODE to control the enabling/ disabling of ICF services based on exact matches between URL patterns rather than broad matches. This ensures that nodes that are not required are not inadvertently enabled by the activation of related nodes. The Note improves controls for services with known security vulnerabilities and public services that do not require any authentication.

Finally, other important patches include Note 2104357 that deals with a potential bypass of URL filters in the ICM and Web Dispatcher, and Note 2114025 that contains instructions for removing a backdoor in the Content Server caused by a hardcoded user.

Appendix: SAP Security Notes, August 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	850306	BC-DB-ORA	Oracle Critical Patch Update Program
HIGH	1562697	BC-MID-RFC	Authorization group for trust relationship
HIGH	2205421	BC-MID-RFC	Update 1 to Security Note 1997734
HIGH	2205521	BC-MID-RFC	Update 1 to Security Note 1562697
HIGH	2175928	HAN-DB-ENG-TXT	Potential remote termination of running processes in SAP HANA text engine
HIGH	2175991	EP-PIN-TOL	Unauthorized modification of displayed content in Theme Integrity Test
HIGH	2037304	SV-SMG-SDD	Lacks proper input validation in SDCC Download Function Module
HIGH	2182154	EP-KM-TLS-XFB	Unauthorized modification of stored content in XMLForms Preview
HIGH	2182842	BC-CUS-TOL-TME	Potential information disclosure relating to SAP Customizing
HIGH	2152227	MOB-ONP	SAP Mobile Platform XXE vulnerability (import MBO applications)
HIGH	2152669	MOB-AFA	Multiple vulnerabilities in SAP Afaria Server
HIGH	2168485	EP-PIN-PSL	XXE Vulnerability in Landscape System Configuration
HIGH	2169391	EP-PIN-NAV-AFP	Reflected File Download vulnerability in AFPServlet
HIGH	2173184	EP-PDK-HBJ	XSS Vulnerabilities in HTMLB
HIGH	2174357	EP-KM-CM	Reflected File Download Vulnerability in KM Documents Servlet
HIGH	2090013	BC-JAS-SEC	Unauthorized modification of displayed content in NetWeaver logon application
HIGH	1997734	BC-MID-RFC	Missing authorization check in RFC runtime
HIGH	1694057	PLM-CFO	Unauthorized modification of displayed content in PLM-CFO(3)
HIGH	2201881	PLM-CFO	Update 1 for Security Note 1694057
HIGH	2183624	HAN-DB-SEC	Potential information leakage using default SSFS master key in HANA
MEDIUM	1777867	XX-PROJ-FI-CA	Potential SQL injection in FI-CA

Appendix: SAP Security Notes, August 2015 Cont.

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2028525	FI-LA	Missing authorization check in FI-LA
MEDIUM	2178356	BC-BMT-BPM-DSK	Missing authorization check in BPM
MEDIUM	2125623	BC-CCM-SLD-REG	Potential remote termination of running processes in BC-CCM-SLD-REG
MEDIUM	2176128	HAN-AS-XS	Potential information disclosure relating to server information
MEDIUM	2180403	BC-DWB-TOO-DBG	Potential information disclosure relating to ABAP Debugger
MEDIUM	2182768	BC-MID-ICF	Too Many http Services Are Activated
MEDIUM	2185409	BC-EIM-ESH	Potential information disclosure relating to passwords
MEDIUM	2187823	CA-WDE	Remote exploit of secondary configuration variables in Apache Cordova of WebIDE
MEDIUM	2192982	BC-SEC-SSL	Potential information disclosure relating to TLS 1.1/1.2
MEDIUM	2193318	MOB-SDK-KAP	Remote exploit of secondary configuration variables in Apache Cordova on Android
MEDIUM	2104357	BC-CST-IC	Bypass of Filter in SAP Internet Communication Manager
MEDIUM	1973081	BC-ABA-SC	XSRF vulnerability: External start of transactions with OKCode
MEDIUM	1830797	BC-MID-ICF	Missing authorization check in BC-MID-ICF
MEDIUM	2157458	BC-MID-ICF	Potential information disclosure relating to Internet Communication Framework
MEDIUM	2165583	HAN-DB	SAP HANA secure configuration of internal communication
MEDIUM	2114025	BC-SRV-KPR-CS	Hard-coded credentials in SAP Content Server
MEDIUM	2091403	BC-MID-ICF	Directory traversal in BC-MID-ICF
MEDIUM	2093939	BC-XI-CON-AXS	Potential information disclosure relating to remote system
MEDIUM	2077857	SD-BIL	Potential disclosure of persisted data in SD-BIL
MEDIUM	2032811	PY-PH	Directory traversal in PY-PH
MEDIUM	2155978	XX-CSC-GR-FI	Potential disclosure of persisted data in Greek FI localization
MEDIUM	2181460	BC-XI-IBC	Unauthorized usage of application functionality in SAP Exchange Infrastructure
LOW	2148905	HAN-AS-XS	Potential information disclosure relating to passwords in SAP Web Dispatcher trace files

LAYER SEVEN SECURITY

Layer Seven Security empowers organizations 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