Layer Seven Security

ADVISORY

SAP Security Notes

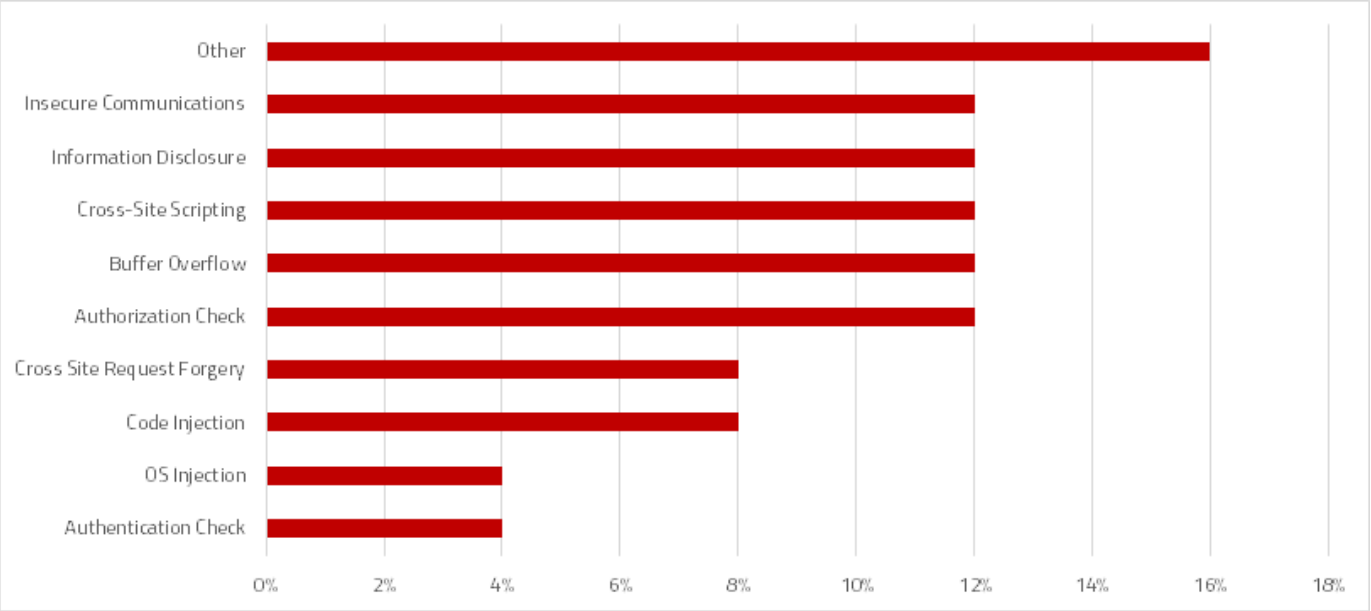
November 2015

SAP Security Notes

November 2015

Similar to the patches released for the Download Manager in October, SAP issued a series of fixes for the Note Assistant in November in response to disclosures performed by an external security researcher that did not follow standard disclosure protocols. The Note Assistant (transaction SNOTE) is used to download and implement software corrections from SAP. This is performed using the SAPOSS RFC connection. The patches address vulnerabilities related to the RFC communication link between client systems and SAP used by SNOTE. Note 2235514 includes corrections to prevent attackers from changing the standard RFC destination. This will prevent attackers from exploiting an existing weakness in SNOTE that could lead the application to inadvertently connect to attacker-controlled servers. Note 2235513 deals with the risk that attackers may be able to exploit the RFC callback mechanism to execute remote enabled function modules in the calling system. This is especially a risk with OSS connections that are configured with privileged users. Callbacks should be rejected for the SNOTE function module SCWN_NOTE_DOWNLOAD. Note 1686632 provides instructions for activating positive whitelists for RFC callbacks. Lastly, 2235515 improves logging for the Note Assistant to ensure that the RFC destination used to download Notes is recorded in the log entry for each correction.

Note 2165583 recommends encrypting internal service communications for SAP HANA. Internal communications should be protected just as strongly as external communications. This will guard against insider threats and provide an additional layer of defense in the event of a network breach. Guidance for configuring transport



SAP Security Notes by Vulnerability Type

layer encryption for internal services are documented in the Master and Security Guides for SAP HANA.

Note 2240274 removes support for Base64 and DES algorithms used to encrypt passwords in SAP Manufacturing. The encoding schemes are widely acknowledged to be insecure and provide minimal protection for sensitive data. The Note recommends the use of the more secure 3DES algorithm.

Finally, Note 2197100 provides instructions for removing a high risk OS injection exploit performed by calling the function module SCTC_REFRESH_EXPORT_USR_CLNT using the background processing transaction SM37. The instructions include controlling access to the authorization objects S_DEVELOP, S_C_FUNCT and S_DATASET.

Appendix: SAP Security Notes, November 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2235513	BC-UPG-NA	External RFC callback to customer systems in SNOTE
HOT NEWS	2235514	BC-UPG-NA	Standard RFC destination for note download can be overridden
HOT NEWS	2235515	BC-UPG-NA	Insufficient logging in SNOTE
HIGH	2194572	EP-PIN-PRT	Unauthorized modification of displayed content in StringBufferPoolMonitor
HIGH	850306	BC-DB-ORA	Oracle Critical Patch Update Program
HIGH	1507735	IS-M	Unauthorized use of application functions in IS-Media
HIGH	2198580	BC-ABA-LA	Code injection vulnerability in ABAP
HIGH	2238619	MFG-PCO	Potential remote termination of running processes in SAP Plant Connectivity
HIGH	2221082	CA-WUI-APF	Unauthorized use of application functions in WEBCUIF and CRMUIF
HIGH	2162829	BW-EI-APD	Code injection vulnerability in BW-EI-APD
HIGH	2237846	BC-ESI-UDDI	Update 1 to Security Note 1322098
HIGH	2197100	BC-INS-TC-CNT	OS injection through call of function module by SM37
HIGH	2120370	BI-BIP-AUT	Update 1 to Security Note 2001109
HIGH	2001109	BI-BIP-AUT	Potential information disclosure relating to BI-BIP-AUT
MEDIUM	2201796	BC-JAS-SEC-LGN	Unauthorized modification of displayed content in Authentication framework
MEDIUM	2185273	BW-WHM-DST-RDA	Missing authorization check in the monitor for real-time data acquisition (RDA)
MEDIUM	2165583	HAN-DB	SAP HANA secure configuration of internal communication
MEDIUM	2240274	MFG-MII	SAP MII uses Base64 and DES for securing passwords
MEDIUM	2235795	BC-CCM-PRN	Potential information disclosure relating to SAP Cloud Print Manager for S/4HANA Cloud Edition
MEDIUM	2223008	BC-IAM-SL	Incorrect Signature Check in DSA Algorithm
MEDIUM	2218957	BC-SRV-FP	Potential remote termination of running processes in Forms Infrastructure
MEDIUM	2218411	BC-SRV-FP	Potential remote termination of running processes in Adobe Document Services
MEDIUM	2043119	FIN-FSCM-LP	Missing authorization check for user exits in Liquidity Planner
MEDIUM	1744879	BC-FES-CTL	Unauthorized modification of stored content in Data Provider
LOW	412309	CRM-IPC	Authorization profile RFC user for IPC

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