ADVISORY

Layer Seven Security

SAP Security Notes

March 2016

SAP Security Notes

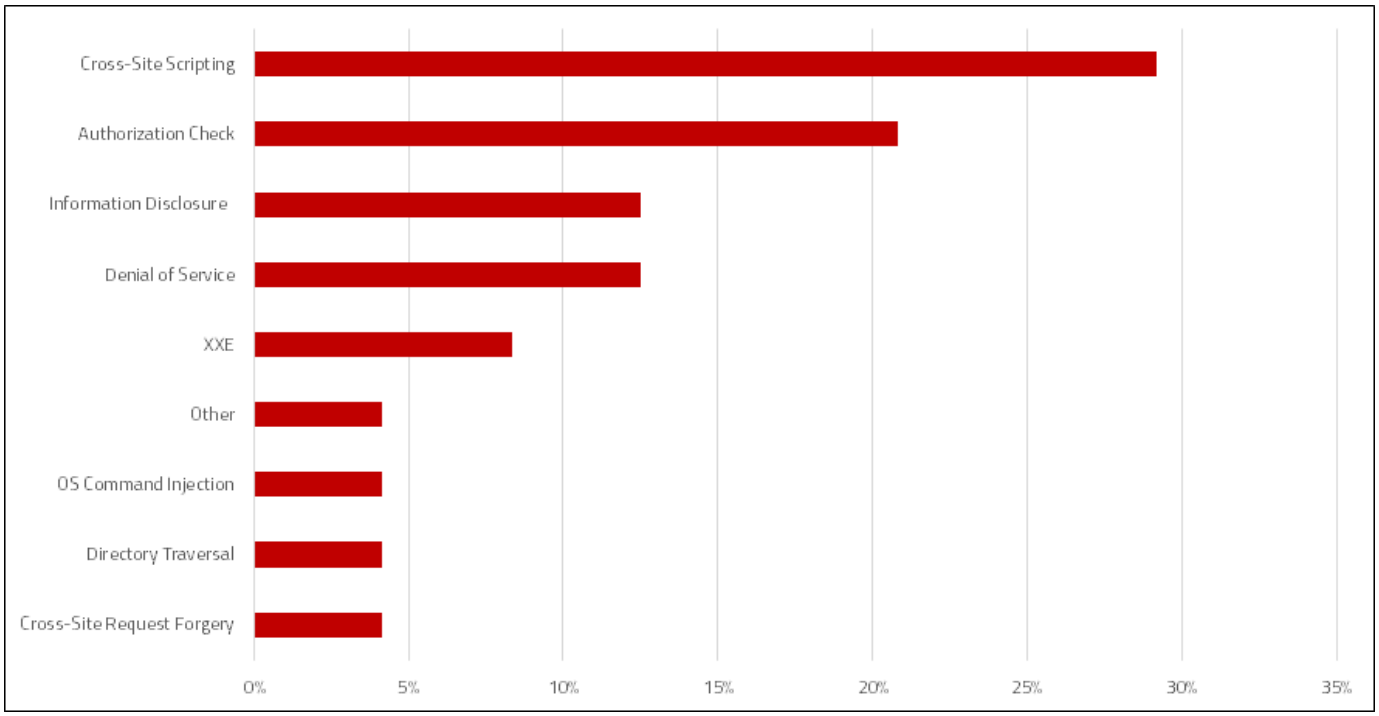
March 2016

Note 2260344 addresses a critical OS command execution vulnerability impacting several function modules used by Central Technical Configuration (CTC). CTC is a post-installation service in SAP NetWeaver that is used to perform basic configuration tasks such as initializing software and application components, creating functional units, and establishing RFC and other connections. Note 2260344 contains manual corrections for removing the ability to execute arbitrary operating system commands through the following function modules using transaction SE37:

SCTC_PREPARE_CHECK_CAPACITY
SCTC_REFRESH_CHECK_ENV
SCTC_REFRESH_CONFIG_CTC
SCTC_REFRESH_EXPORT_TAB_COMP
SCTC_REFRESH_IMPORT_USR_CLNT
SCTC_REORG_SPOOL
SCTC_TMS_MAINTAIN_ALOG

The OS commands can be performed using the privileges of the CTC service and can lead to the complete compromise of the SAP file system, source code, and database. The manual tasks required to remove the vulnerability require some experience of working with ABAP development objects to redevelop the impacted function modules.

SAP also released high priority Notes for vulnerabilities that were demonstrated at the Troopers Security Conference in March. Note 2259547 delivers a kernel patch for a denial of service vulnerability in JSTART, the Java Startup Framework used to start, monitor and stop Java instances and processes. Note 2256185 deals with a similar vulnerability in the Internet Communication Manager (ICM), responsible for managing Web-based communication



SAP Security Notes by Vulnerability Type

between clients and SAP servers. In both cases, the DoS is provoked by a resource exhaustion condition.

Other important patches include Note 2213128 which provides switchable authorization checks for RFC-enabled function modules supporting batch management in SAP ERP, Note 2258786 which removes a vulnerability in the SAP Web Administration Interface that could be exploited to disclose sensitive information related to installed products and versions and the system landscape, and lastly, Note 2282338 which improves cryptographic encoding for logon data stored in the SAP Download Manager.

Appendix: SAP Security Notes, March 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2260344	BC-INS-TC-CNT	OS command injection vulnerability in SCTC_* Function modules
HIGH	2256185	BC-CST-IC	Potential denial of service in SAP Internet Communication Manager
HIGH	2259547	BC-JAS-SF	Potential denial of service in jstart
HIGH	2071329	IS-A-DP	Update 1 to security note 1676754
HIGH	1676754	IS-A-DP-VMS	Unauthorized modification of BSP in Webdocuments
MEDIUM	2281095	PLM-ECC	Missing authorization check in ECTR
MEDIUM	1943280	XX-CSC-RU-FI	Missing authorization check in XX-CSC-RU-FI
MEDIUM	2213128	LO-BM-GBT	Switchable authorization checks for RFCs in GBT integration component GBTRINT in ERP
MEDIUM	2258786	BC-CST-IC	Potential information disclosure relating to SAP Web Administration Interface
MEDIUM	2255990	EP-PIN-RTC	Potential information disclosure relating to Real Time Collaboration Chat
MEDIUM	2253850	EP-PIN-RTM	XML External Entity vulnerability in RTMF
MEDIUM	2204581	BI-BIP-BIW	Unauthorized modification of displayed content in BI Workspace - custom JS
MEDIUM	2260895	BI-RA-EXP	Potential information disclosure relating to Explorer web application server
MEDIUM	2282338	XX-SER-SAPSMP-SDM	SAP Download Manager Password Weak Encryption
MEDIUM	2269315	BC-SEC-LGN	Missing authorization check in OAuth2 Server Runtime
MEDIUM	2238765	EP-PIN-NAV	Unauthorized modification of displayed content in CacheAPITester and findMerge
MEDIUM	2238375	EP-PIN-NAV	Unauthorized modification of displayed content in NavigationURLTester
MEDIUM	2235994	BC-INS-CTC	Untrusted XML input parsing possible in Configuration Wizard
MEDIUM	2234971	BC-JAS-ADM-MON	Directory traversal in AS Java Monitoring
MEDIUM	2219896	EP-PIN-PB-PRT	Unauthorized modification of stored content in Portal Page Builder
MEDIUM	2210310	EP-PIN-NAV-AFP	Unauthorized use of application functions in NavigationServlet
LOW	2133144	LE-WM-VAS	Missing whitelist check in LE-WM-VAS LE-TRM and LE-YM
LOW	2189174	BC-CST-MS	Unauthorized modification of displayed content in message server
LOW	2223688	BC-CST-MS	Potential denial of service in Message Server

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