ADVISORY

Layer Seven Security

SAP Security Notes

January 2017

SAP Security Notes

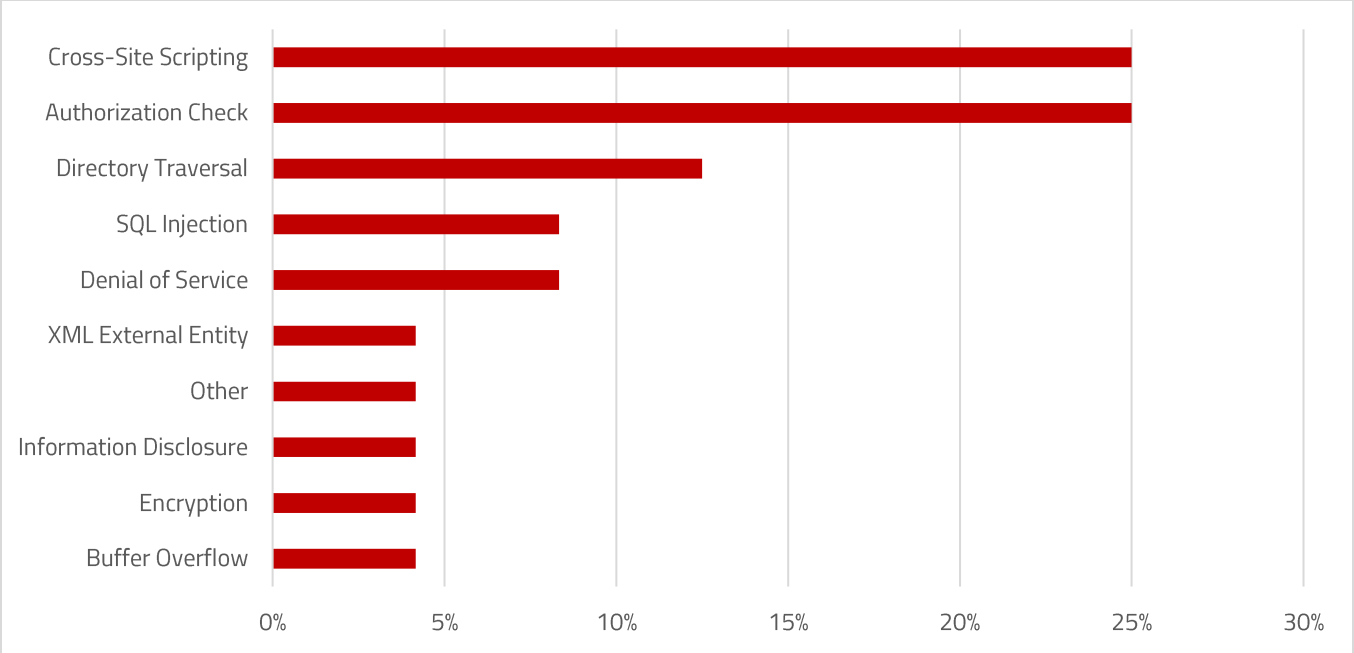
January 2017

Hot News Note 2407862 deals with a highly dangerous buffer overflow vulnerability in Sybase Software Asset Management (SySAM) that scores almost 10/10 using the Common Vulnerability Scoring System. SySAM performs license management for products such as ASE, ESP, PowerDesigner and the Replication Server.

The vulnerability arises from the Flexera Flexnet Publisher software bundled in SySAM. The third party software is bundled in products provided not only by Sybase, but vendors such as Intel, Cisco, HP, Adobe, RSA and Siemens.

Flexnet Publisher is vulnerable to a stack buffer overflow vulnerability that could enable attackers to execute arbitrary code remotely and without authentication. Since the code could provoke a crash in the Vendor Daemon which performs license control in software products, it could lead to a denial of service in SySAM and products that rely on SySAM. This explains the extremely high CVSS score of the vulnerability.

According to Flexera, a patch for the vulnerability was made available to vendors in November 2015. It is not clear if this included SAP. The vulnerability was published in the NIST National Vulnerability Database (NVD) shortly thereafter in February 2016. Despite the criticality of the vulnerability, a correction for SySAM was only made available in January 2017. Customers are advised to download and install SySAM 2.4 to apply the correction.



SAP Security Notes by Vulnerability Type

Note 2389042 deals with a similar denial of service vulnerability in SAP Single Sign-On (SSO) which could interrupt the availability of SAP services for users. The SSO Authentication Library should be patched to the latest patch level specified in the Note.

Note 2407696 removes support for the DES encryption algorithm used to secure configuration data in SAP Online Banking 8.3. SAP recommends using stronger algorithms supported by Online Banking including AES and 3DES. Note that AES is more efficient in software implementations than 3DES since 3DES was designed for hardware implementations.

Appendix: SAP Security Notes, January 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2407862	BC-SYB-SAM	Multiple buffer overflows in Flexera Flexnet Publisher (CVE-2015-8277) Sybase Asset Management
HIGH	2389042	BC-IAM-SSO-OTP	Denial of service (DOS) in SAP Single Sign On
MEDIUM	2347077	CRM-MKT-MPL-TPM-IMP	Cross-Site Scripting (XSS) vulnerability in IMP planning table / CRM-MKT-MPL-TPM-IMP
MEDIUM	2355398	SD-BIL-IV-CB	Missing Authorization check in RFC function module
MEDIUM	2355339	SD-BIL-IV-CB	Directory Traversal Vulnerability in FSB
MEDIUM	1541716	BC-DOC-TTL	Potential Denial of Service in translation tools funct.
MEDIUM	2407696	FS-OCB-GEN-SEC	Removal of DESEncrypt class from SAP Online Banking 8.3
MEDIUM	2361633	BI-BIP-SL-SDK	SQL Injection vulnerability in SAP Business Intelligence platform
MEDIUM	2378090	SV-SMG-SDD	Missing Authorization check in SAP Solution Manager
MEDIUM	2389578	BC-ABA-LA	Directory Traversal vulnerability in File Interface in SAP Netweaver
MEDIUM	2370876	BC-JAS-ADM-LOG	Directory Traversal vulnerability in SAP NetWeaver Log Viewer
MEDIUM	2369469	EP-PIN-NAV	Cross-Site Scripting (XSS) vulnerability in SAP Enterprise Portal Navigation
MEDIUM	2407670	BC-DWB-AIE-SRC	Missing Authorization check in ABAP Development Tools
MEDIUM	2341302	EP-PIN-RTC	Cross-Site Scripting (XSS) vulnerability in SAP Enterprise Portal Real Time Collaboration
MEDIUM	2356504	BC-ESI-UDDI	SQL Injection vulnerability in SAP Netweaver UDDI Server
MEDIUM	2347439	EP-VC	Missing XML Validation vulnerability in SAP Netweaver Visual Composer
MEDIUM	2378448	IS-DFS-BIT-DIS	Missing Authorization check in SAP ERP Defence Forces and Public Security
MEDIUM	2378417	IS-DFS-BIT	Missing Authorization check in SAP ERP Defence Forces and Public Security
MEDIUM	2377626	EP-PIN-TOL	Cross-Site Scripting (XSS) vulnerability in SAP Enterprise Portal Theme Editor
MEDIUM	2376524	IS-DFS-BIT-DIS	Missing Authorization check in SAP ERP Defence Forces and Public Security

Appendix: SAP Security Notes, January 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2372204	EP-PIN-TOL	Cross-Site Scripting (XSS) vulnerability in SAP Enterprise Portal Theme Editor
MEDIUM	2372183	EP-PIN-TOL	Cross-Site Scripting (XSS) vulnerability in SAP Enterprise Portal Theme Editor
MEDIUM	2407351	CRM-MKT-MPL-CBP	Unrestricted File Upload vulnerability in Customer Business Planning application
LOW	2374348	BC-SYB-SQA	Information Disclosure in DBISQL affecting SAP SQL Anywhere, SAP ASE and SAP IQ

LAYER SEVEN SECURITY

Layer Seven Security serve customers worldwide to harden, patch and monitor SAP systems against cyber threats using SAP Solution Manager

Address

99 Hudson Street
5th Floor
New York, NY 10013
United States

Web

www.layersevensecurity.com

Email

info@layersevensecurity.com

Telephone

1-647-964-7370