ADVISORY

Layer Seven Security

SAP Security Notes

August 2016

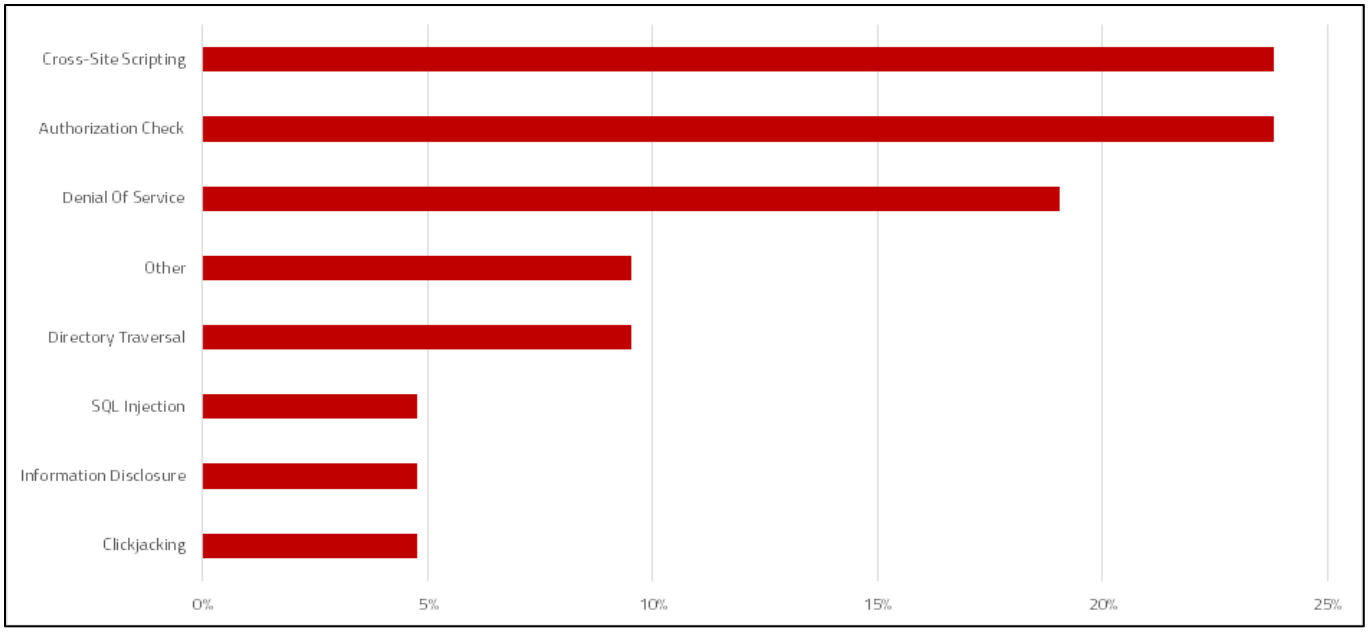
SAP Security Notes

August 2016

Note 2319506 addresses a blind SQL injection vulnerability in Database Monitors for Oracle. The vulnerability impacts all versions of SAP Basis and rates extremely high on the impact scale using the common vulnerability scoring system. Content-based and time-based blind SQL injection is used by attackers to determine when input is interpreted as a SQL statement. The results are used to fingerprint databases, build database schemas and escalate attacks.

The blind SQL injection vulnerability in the Database Monitors is caused by improper validation of user-supplied input in the function modules STUO_GET_ ORA_SYS_ TABLE and STUO_GET_ORA_SYS_TABLE_ 2. The modules are used to read Oracle system tables containing sensitive data including database instances and logical names for database connections. Corrections for the vulnerability are included in support packages for relevant SAP Basis versions detailed in Note 2311011.

Note 2313835 deals with a high risk denial of service vulnerability in the Internet Communication Manager (ICM). The ICM manages client-server communication using Web protocols such as HTTP, HTTP, and HTTPS. For NetWeaver Application Server Java, the ICM also manages communications based on the proprietary SAP P4 protocol. Note 2313835 provides kernel patches for DOS and DDOS attacks targeted at the P4 port of AS Java that could lead to service disruptions caused by resource exhaustion.



SAP Security Notes by Vulnerability Type

Note 2142551 delivers a framework for protecting AS ABAP against clickjacking attacks. This includes a client-dependent positive whitelist maintained in the HTTP_WHITELIST table. The key data to be maintained for each entry in the whitelist is entry_type and host. The recommended value setting for entry_type is 30 to enable clickjacking protection. Trusted hosts and domains should be defined in the host field.

Note 2012284 provides corrections to extend virus scanning to objects created by Knowledge Provider, a document and content management service within NetWeaver Application Servers.

Appendix: SAP Security Notes, August 2016 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2319506	BC-CCM-MON-ORA	SQL Injection vulnerability in Database Monitors for Oracle
HIGH	2313835	BC-CST-IC	Denial of service (DOS) in SAP Internet Communication Manager
HIGH	1477597	EP-KM-CM	Unauthorized modification of stored content in NW KMC
HIGH	2351001	EP-KM-CM-SEC	Update 1 to security note 1477597
HIGH	1718230	BI-BIP-BIW	Unauthorized modification of displayed content in StratBuild
HIGH	2224249	EP-PIN-DNT	Unauthorized modification of stored content in ConfigEditor
MEDIUM	2294866	BC-JAS-JMS	Missing proper authorization checks in JMS Provider Service
MEDIUM	2069820	BW-BEX-ET	Missing authorization check in BW-BEX-ET
MEDIUM	2292714	BC-ABA-LA	Denial of service (DoS) vulnerability in Memory Snapshot Creation
MEDIUM	2142551	BC-WD-ABA	Whitelist service for Clickjacking Framing Protection in AS ABAP
MEDIUM	2012284	BC-SRV-KPR-CMS	Knowledge Provider passes incorrect status of virus scan to the content server
MEDIUM	2307947	BC-XI-IS-WKB	Information Disclosure in Runtime Workbench
MEDIUM	2249634	BI-BIP-INV	Cross-Site Scripting (XSS) vulnerability in BIWorkspace
MEDIUM	2327384	BC-INS-TLS	Race condition upon file permission change in SAPCAR
MEDIUM	2317096	FIN-FSCM-TRM-TM	Missing Authorization check in Transaction Manager

Appendix: SAP Security Notes, August 2016 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2312966	AP-MD-BP	Directory Traversal vulnerability in Business Partner
MEDIUM	2296909	BC-BMT-BPM-DSK	Denial of service (DOS) vulnerability in BPM
MEDIUM	2317358	SCM-YL	Missing Authorization check in SAP Yard Logistics
LOW	2250863	XX-CSC-IN-MM	Missing authorization check in XX-CSC-IN-MM
LOW	2280371	BC-JAS-COR	Directory Traversal Vulnerability in a Telnet Command
LOW	2312905	BC-INS-TLS	Denial of service (DOS) in SAPCAR

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

Layer Seven Security offers no specific guarantee regarding the accuracy or completeness of the information presented, but the professional staff of Layer Seven Security makes every reasonable effort to present the most reliable information available to it and to meet or exceed any applicable industry standards.