Layer Seven Security

ADVISORY

SAP Security Notes

July 2016

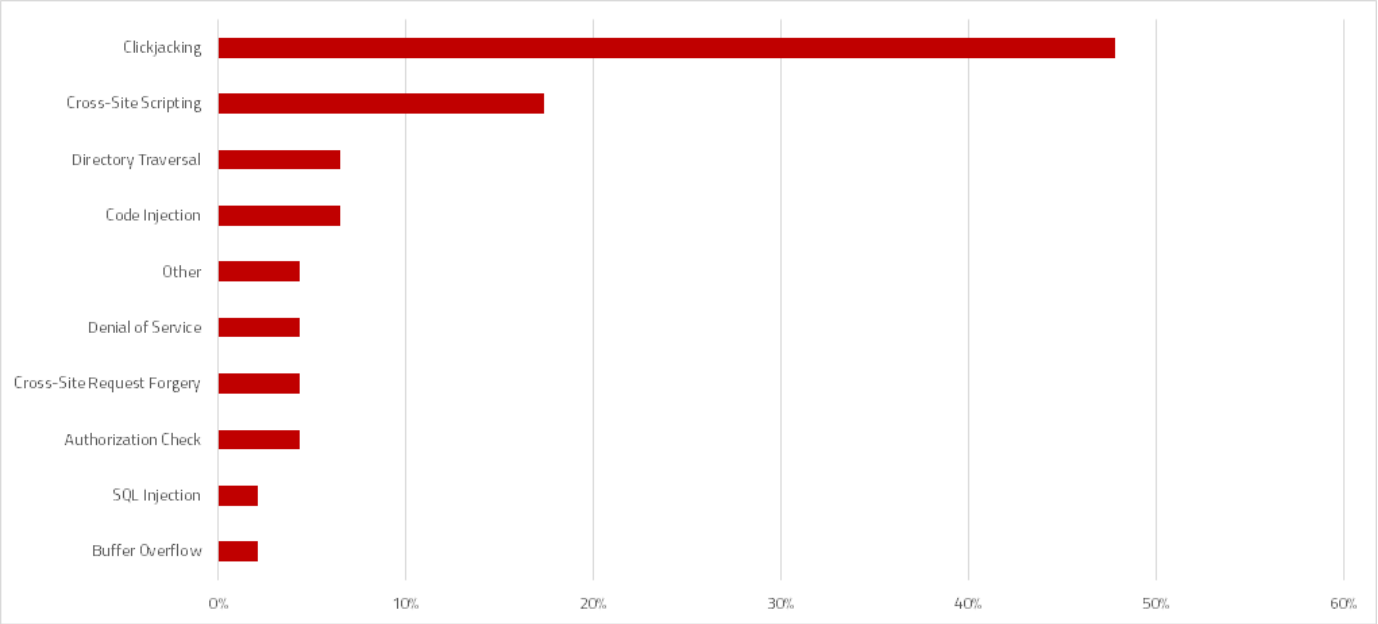
SAP Security Notes

July 2016

Hot News Note 2301837 patches a dangerous code injection vulnerability in SAP Solution Manager. The vulnerability is due to a programming error in the PING_HOST method in specific ABAP objects. Since the method is obsolete, the correction instructions packaged in the Note recommend deleting the relevant code block. The vulnerability carries a CVSS score of 9.9/ 10.0 and rates especially high in terms of the exploit range of the attack vector and the impact on data confidentiality and integrity for successful exploits.

SAP released a series of Notes in July to protect supported user interfaces against UI redress exploits, also known as clickjacking attacks. Clickjacking occurs when users are deceived into clicking on buttons or other objects in web pages with multiple layers. The clicks are routed to applications and domains controlled by attackers. This can lead users to inadvertently execute malicious programs or functions or disclose sensitive information through keystrokes entered within frames that are often invisible to the user.

There are several methods for combating clickjacking attacks. X-Frame Options in HTTP response headers can be configured to enable browsers to deny rendering frames or other objects in pages or allow rendering from sites from specific domains or within the same domain as the original page. However, this approach is not suitable for most NetWeaver integration scenarios. Other options include frame busting. This is often used by web applications to prevent the rendering of pages within frames.



SAP Security Notes by Vulnerability Type

SAP has adopted a multi-pronged approach to secure inter-frame communication. Note 2319727 provides examples for countermeasures covering multiple scenarios. This includes disallowing embedding by others systems altogether and allowing embedding for trusted systems or domains. The protection framework delivered by SAP includes a positive whitelist to maintain permitted systems and domains.

Notes 2194572, 2182154, 2224249 and 2228405 address high risk cross-site scripting vulnerabilities in components of the Enterprise Portal. This includes the Portal runtime environment, ConfigEditor, and XMLForms Preview.

Finally, Note 2234971 removes a directory traversal vulnerability in AS Java that could be exploited to read arbitrary files on Java servers and lead to the disclosure of sensitive information.

Appendix: SAP Security Notes, July 2016

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2301837	SV-SMG-ADM	Code Injection vulnerability in SAP Solution Manager
HIGH	2194572	EP-PIN-PRT	Unauthorized modification of displayed content in StringBufferPoolMonitor
HIGH	2182154	EP-KM-TLS-XFB	Unauthorized modification of stored content in XMLForms Preview
HIGH	2224249	EP-PIN-DNT	Unauthorized modification of stored content in ConfigEditor
HIGH	2228405	EP-PIN-CS	Unauthorized modification of stored content in EPCF Loader Tester
HIGH	2169391	EP-PIN-NAV-AFP	Reflected File Download vulnerability in AFPServlet
HIGH	1678072	BC-SRV-KPR	Update #1 to Security Note 1579673
HIGH	1727640	BC-SEC	Update 1 to security note 1520101
HIGH	1542033	BC-CCM-FIL	Update #1 for security note 1497003
HIGH	1724922	BC-WD-JAV	Update 1 to Security Note 1653474
HIGH	2245398	XX-PART-ADB-IFM	Java Deserialization Vulnerability in Adobe Interactive Forms
HIGH	2330839	BC-SYB-OS	Denial of service (DOS) in multiple SAP Sybase products
MEDIUM	2234971	BC-JAS-ADM-MON	Directory traversal in AS Java Monitoring
MEDIUM	2240548	BC-CCM-SLD-JAV	Unauthorized use of application functions in SLD
MEDIUM	2218411	BC-SRV-FP	Potential remote termination of running processes in Adobe Document Services
MEDIUM	2339506	IS-U-CS-ISS	Whitelist based Clickjacking Framing Protection in Utility Customer E-Services
MEDIUM	2339167	FIN-FSCM-BD	Whitelist based Clickjacking Framing Protection in FSCM Biller Direct
MEDIUM	2338446	MFG-MII	Clickjacking Framing Protection in MII
MEDIUM	2337225	PE-LSO-CP	Clickjacking vulnerability in LSO Content Player
MEDIUM	2245332	CA-UI5-ABA	Automatic usage of Whitelist Service for Clickjacking Framing Protection in SAPUI5 Apps
MEDIUM	2263656	EP-PDK-HBJ	Whitelist based Clickjacking Framing Protection in HTMLB Java
MEDIUM	2333957	CA-UI2-INT-FE	Whitelist based Clickjacking Framing Protection in SAP Fiori Launchpad for NW AS ABAP
MEDIUM	2329738	BC-SYB-ASE	Unrestricted File Creation vulnerability in SAP ASE
MEDIUM	2142551	BC-WD-ABA	Whitelist service for Clickjacking Framing Protection in AS ABAP
MEDIUM	2286679	BC-WD-JAV	Whitelist Service API required for the Clickjacking Framing Protection in JAVA at the framework or application level
MEDIUM	2290512	BI-BIP-INV	Cross-Site Scripting (XSS) vulnerability in BI Platform and BI Launch Pad

Appendix: SAP Security Notes, July 2016 Cont.

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2290783	BC-JAS-WEB	Whitelist based Clickjacking Framing Protection for Java Server Pages
MEDIUM	2295238	BC-CST-STS	Memory Corruption vulnerability in Startup Service
MEDIUM	2297227	CRM-ISA	Whitelist based Clickjacking Framing Protection in CRM-ISA
MEDIUM	2303032	BC-WD-ABA	Cross-Site Scripting (XSS) vulnerability in CL_WDR_CLIENT_SSR_LS
MEDIUM	2309079	FS-CML	Missing authorization check in FS-CML
MEDIUM	2315788	EP-PIN-FPN	Denial of service (DOS) in Enterprise Portal: Federated Portal Network
MEDIUM	2319172	BC-FES-ITS	Whitelist based Clickjacking Framing Protection in SAP GUI for HTML
MEDIUM	2319192	BC-BSP	Whitelist based Clickjacking Framing Protection in BSP
MEDIUM	2319184	CA-UI5-COR	Whitelist based Clickjacking Framing Protection in SAPUI5
MEDIUM	2319174	BC-FES-BUS-HTM	Whitelist based Clickjacking Framing Protection in NWBC for HTML
MEDIUM	2319727	BC-SEC	Clickjacking protection framework in SAP Netweaver AS ABAP and AS Java
MEDIUM	1872800	BC-WD-ABA	Whitelist based Clickjacking Framing Protection in Web Dynpro ABAP
MEDIUM	2321240	HAN-DP-LTR	Missing Authorization check in LT Replication Server (SLT)
MEDIUM	2169722	EP-PIN-AI	Whitelist based Clickjacking Framing Protection in Enterprise Portal
MEDIUM	2169860	BC-WD-JAV	Whitelist based Clickjacking Framing Protection in Web Dynpro Java
MEDIUM	2170590	BC-WD-JAV	Whitelist service for Clickjacking Framing Protection in AS JAVA
MEDIUM	2209907	BW-BEX-ET-WJR-RT	Whitelist based Clickjacking Framing Protection in BW reports
MEDIUM	2157355	XX-CSC-RO-FI	SQL Injection vulnerability in XX-CSC-RO-FI
LOW	1540408	EHS-SAF	Update #1 for security Note 1505368
LOW	2244161	WEC-FRW	Clickjacking Protection in Web Channel Experience Management (WCEM)

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