ADVISORY

Layer Seven Security

SAP Security Notes

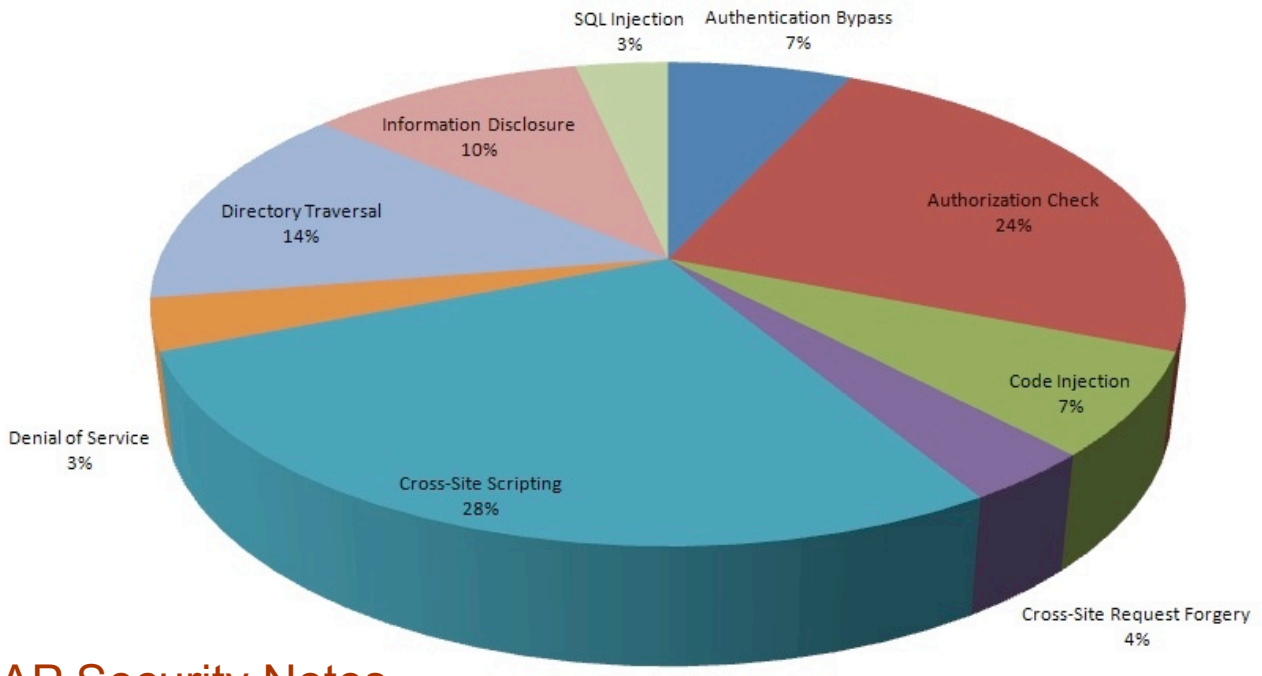
September 2012

SAP Security Notes

September 2012

September witnessed the release of an important patch for the E-Recruiting application of Human Capital Management (HCM). Also known as PA-ER, E-Recruiting is used to manage the entire process chain in recruiting, including everything from identifying and meeting resource needs to retention and succession planning. It includes functions for the electronic screening, filtering, and ranking of candidates, interfacing with external systems such as job boards, and synchronizing with HR master data through ALE (Application Link Enabling) and Process Integration (PI). E-Recruiting requires a complex technical landscape with connections not only to back-end ERP systems, but links to components such as the Enterprise Portal, TREX for text and metadata search and mail servers for messaging. It also requires numerous services in the Internet Communication Framework (SICF) for calling remote function modules using the RFC protocol. Both of these areas present a formidable security challenge. Having said that, last month's patch delivered through Note 1738828 dealt neither with technical nor communication security, but with a missing authorization check that could lead to the escalation of privileges for authenticated users. The Note carried SAP's highest priority level and appeared to relate to missing or inadequately defined checks for the authorization object P_RFC_VIEW. This object is used to control access to recruiting data such as candidate information.

SAP also patched a major access flaw in components of the NetWeaver Administrator (NWA) through Note 1668224. NWA is a web-based tool used for landscape-wide monitoring and administration. It includes work centers for managing the security of Java components in the SAP NetWeaver Application Server (AS Java). This includes areas such as authentication through login modules, identity management, key storage and certificate management, log configuration, Message Server parameters and settings, and connections with external virus scanners.



SAP Security Notes by Vulnerability Type

It also includes work centers for operations such as job scheduling and starting/stopping Java instances, services and applications. Note 1668224 recommends the deletion of an obsolete function module in NWA known as SOHMBEANS. The module include objects that enable users to execute OS commands.

E-Recruiting and NWA were not the only targets for patches dealing with critical access issues. Notes 1753376 and 1756978 patched XML signature vulnerabilities affecting Single-Sign-On (SSO) and SAP HANA. XML signatures are a core component of Security Assertion Markup Language (SAML) version 2 and are used to secure and validate SOAP messages. The Notes patch multiple external SAML implementations vulnerable to signature wrapping attacks that could be used to gain access to SAP data and system resources. Such attacks can be also be used to provoke a denial of service.

The final most noteworthy patch released in September deals with a code injection vulnerability affecting version 7.20 of SAP GUI. Attacks through server-side commands against clients have been a long-standing concern in SAP GUI. A well-defined set of security rules in the SAP GUI security module should provide effective protection against such attacks and prevent attackers from gaining control of clients and accessing back-end SAP systems. This will enable checks for server-side attempts to read, overwrite or execute the contents of local files. However, there are methods to circumvent such checks. Note 1678732 patches one such method and given the widespread deployment of SAP GUI, the note should be closely reviewed and applied wherever applicable.

Appendix: SAP Security Notes, September 2012

PRIORITY	NOTE	AREA	DESCRIPTION
1	1738828	PA-ER	Missing authorization check in ERECRUIT
1	1668224	BC-NWA-AA	Delete SOHMBEANS
2	1720634	BW-WHM-DST	Directory traversal in BW-WHM-DST
2	1720999	AP-PRC-PR	Update 1 to Security Note 1531958
2	1722446	CRM-FRW-UI-TAG	Unauthorized modification of displayed content in WEBCUIF
2	1737708	CRM-ISA-SHA	Unauthorized modification of displayed content in CRM-ISA-SH
2	1738564	FIN-FSCM-TRM-TM	Missing authorization check in TM Reporting
2	1741028	XX-PROJ-CDP-016	Unauthorized modification of displayed content in JBM Web
2	1744122	BC-ABA-XML	Untrusted XML Input parsing possible in iXML applications
2	1744747	CRM-ISA-TEC	Unauthorized modification of stored content in CRM-IPC
2	1746943	BC-SEC-SSF	Unauth. modification of displayed content in BSP SAPSIGN
2	1747396	SRM-EBP-TEC-ITS	Unauthorized modification of stored content in Logon screen
2	1749777	BW-BEX-ET-WJR	Unauthorized modification of content displayed in BW
2	1753376	BC-JAS-SEC-LGN	SAML 2.0: possible XML Signature wrapping attack
2	1756978	BC-DB-HDB	SAML 2.0: possible XML signature wrapping attack
2	1576215	BC-CCM-MON-OS	Deletion of an obsolete FM EXE_SAPOSCOL
2	1590175	CRM-MKT-DAM	Unauthorized use of application functions in CRM-MKT-DAM
2	1621534	BC-JAS-SEC-UME	Untrusted XML input parsing possible in SPML Service
2	1678732	BC-FES-GUI	SAP GUI for Windows 7.20: Client Side Remote Execution
2	1693981	BC-SEC-VIR	Unauthorized modification of displayed content
2	1698242	FI-GL-GL-F1	FI: Potential Directory Traversal- Italy(RFIDITVCL)
2	1719102	FIN-FSCM-TRM-TM	Missing authorization check in Treasury
3	1555906	EP-PDK-HBJ	Unauthorized modification of displayed content in HTMLB
3	1635970	BC-XI-CON-AFW-DC	Potential information disclosure relating to passwords
3	1542355	BW-BEX-ET-WJR-RT	BEx Web: Removing DEBUG=X parameter for non-admin users
3	1718378	BW-BEX-OT-BIA	Directory Traversal in Query Snapshot
3	1718408	BW-BEX-OT-DBIF	Directory Traversal in database interface
3	1743359	BC-JAS-ADM-ADM	Update 1 to Security Note 1663799
4	1644896	BC-BMT-BPM-DSK	Missing authorization check in SAP NetWeaver BPM Task Mgmt

Layer Seven Security

Layer Seven Security specialize in SAP security. We serve customers worldwide to protect information assets against internal and external threats and comply with industry and statutory reporting requirements. The company fuses technical expertise with business acumen to deliver unparalleled audit, consulting and vulnerability assessment solutions targeted at managing risks associated with contemporary SAP systems.

Our consultants have an average of ten years of experience in field of SAP security and proficiency in regulatory compliance including Basel II, GLBA, HIPAA, FISMA, PIPEDA, PCI DSS and SOX.

The company is privately owned and headquartered in Toronto, Canada.

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