ADVISORY

Layer Seven Security

SAP Security Notes

August 2012

SAP Security Notes

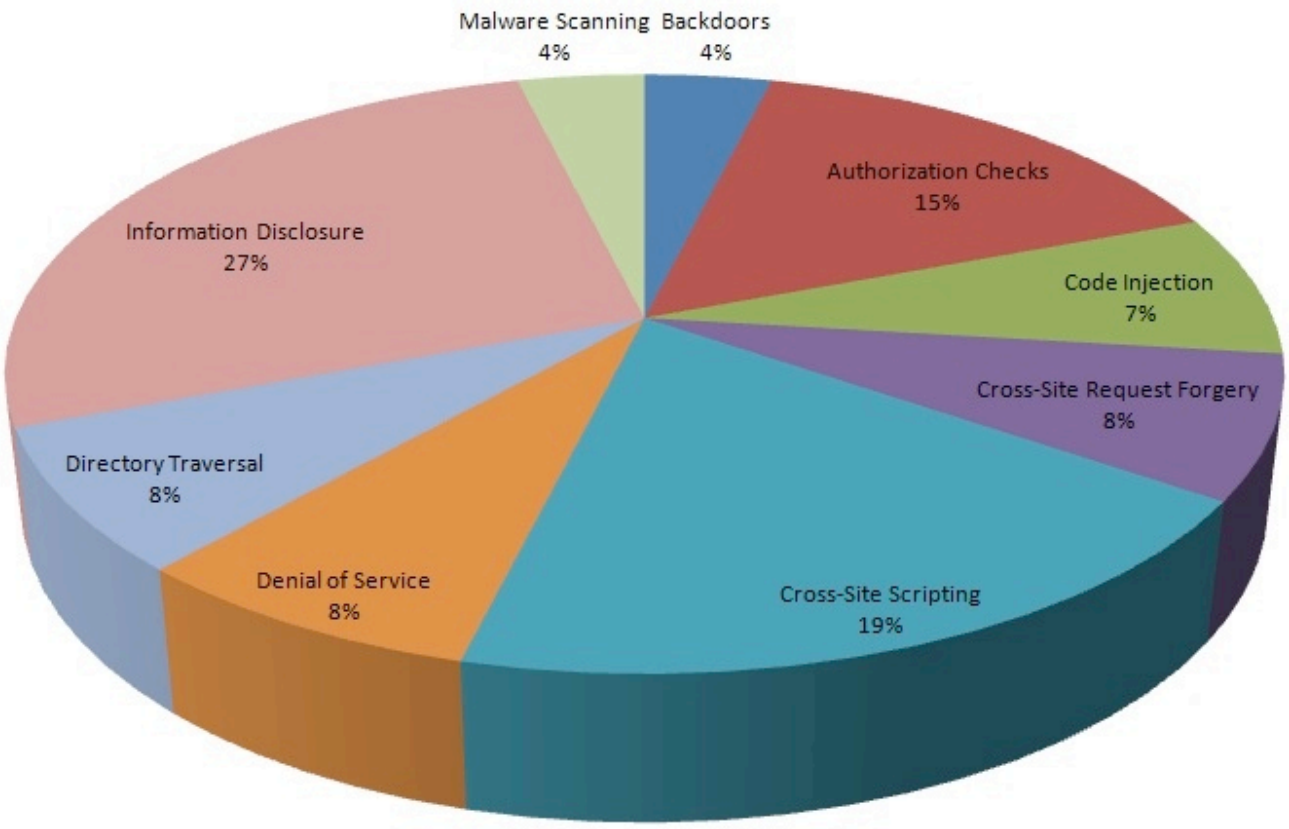
August 2012

SAP released a host of crucial security patches in August. The most important related to missing authorization checks in ST-PI (Note 1727914). ST-PI is a plug-in used to support Basis monitoring services such as EarlyWatch in the Computing Center Management System (CCMS). It includes function modules used for data collection, a SQL trace interpreter that monitors access to database tables, and a control center known as SDCC that collects and manages data related to system performance. SDCC feeds directly into processes used by the SAP Solution Manager to monitor and control SAP landscapes. SAP patched a similar vulnerability in ST-PI in July through Note 1720994. The more recent Note, however, carried a far higher CVSS base score (7.5 compared to 3.5 for the earlier Note). This may be due to the fact that the vulnerability patched in August can be exploited by remote users.

SAP also released a patch for a hardcoded username and password combination in the database supporting certain versions of Billing Consolidation. This is a Java-based application that automates invoice presentment and settlement. It's commonly used as a B2B platform by service providers specializing in process optimization. Billing Consolidation uses connectors to support the electronic exchange of documents between business partners. Note 1715079 patched a vulnerability in the digital signature service of the program.

Note 1677291 introduced a kernel patch for a Denial of Service (DoS) vulnerability in components of the SAP Application Server including the Internet Communication Manager, Web Dispatcher and Message Server. The DoS is triggered by hashtable collision attacks that overload system resources with specific HTTP requests.

Over one quarter of the Security Notes released by SAP in August deal with information disclosure vulnerabilities affecting SAP components such as the



SAP Security Notes by Vulnerability Type

Enterprise Information Management Steward, designed to monitor the integrity of data objects, and SAProuter, an application-level gateway used to control network access to SAP systems. Note 1687334 patched information disclosure vulnerabilities in XML encrypted SOAP messages sent to the NetWeaver AS ABAP. In response to recent research presented at the 18th ACM Conference on Computer and Communication Security (CCS) by Tibor Jager and Juraj Somorovsky, SAP recommends disabling XML encryption in web services and switching to SSL for transport layer protection.

Note 1637451 tackled a crucial vulnerability in the Direct Store Delivery (DSD) area of SAP Logistics. Although the Note carried a relatively low priority level, it dealt directly with a vulnerability that could be exploited by attackers to expose customer credit card data including primary account numbers.

Appendix: SAP Security Notes, August 2012

PRIORITY	NOTE	AREA	DESCRIPTION
1	1727914	SV-SMG-SDD	Missing authorization checks in ST-PI
2	1715079	FIN-FSCM-BC	Hard-coded credentials in Signature Service of SAP Billing C
2	1718230	BI-BIP-BIW	Unauthorized modification of displayed content in StratBuild
2	1718613	BC-UPG-TLS-TLA	Missing authorization check in FM DD_DB_IMIG_CALL_INSTTOOL
2	1718922	BC-BMT-WMD	Potential false redirection in workflow modeler portal
2	1723447	CA-WUI-UI-TAG	Unauthorized modification of displayed content in WEBCUIF
2	1728500	BC-ESI-WS-ABA-RT	Unauthorized use of SOAP-Processor 620
2	1732769	EIM-IS	Potential information disclosure relating to passwords
2	1663732	BC-CST-NI	Potential information disclosure relating to SAProuter
2	1669031	BC-FES-ITS	Deletion of unused classes and update of RFID service
2	1677291	BC-CST	Potential denial of service in Web Application Components
2	1684632	BC-JAS-SEC-WSS	Potential information disclosure XML Encrypted SOAP messages
2	1687334	BC-SEC-WSS	Potential information disclosure XML Encrypted SOAP messages
2	1692988	BC-SRV-COM-FTP	Directory traversal in SFTP modules
2	1699041	XX-CSC-BR-REP	IN86: Potential Directory Traversal
2	1702930	EP-EWP-RT	Enterprise workspaces XSS Encoding Library - StringUtils
2	1705798	IS-A-MON	Missing authorization check in IS-A-MON.
2	1747140	BC-XI-CON-AFW	Update 1 to Security Note 1723641
2	1751530	BC-SRV-KPR-CS	Update 1 to security note 1585767
3	1717391	BC-BMT-WFM-DEF	Code injection vulnerability in BC-BMT-WFM-DEF
3	1732768	EIM-IS	Unauthorized use of application functions in Info. Steward
3	1732771	EIM-IS	Potential information disclosure relating to usernames
3	1734308	BI-BIP-UDT	Potential information disclosure relating to BOE XI3.1 FP5.1
3	1628711	BC-FES-BUS-RUN	Unauthorized modification of NWBC binaries
3	1637451	LE-DSD-DC-DU	Encryption of credit card data in DSD
3	1645844	BC-XI-IBC	PI SEC: Missing authorization check in Integration Builder

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