


Layer Seven Security

SAP Security Notes
October 2012



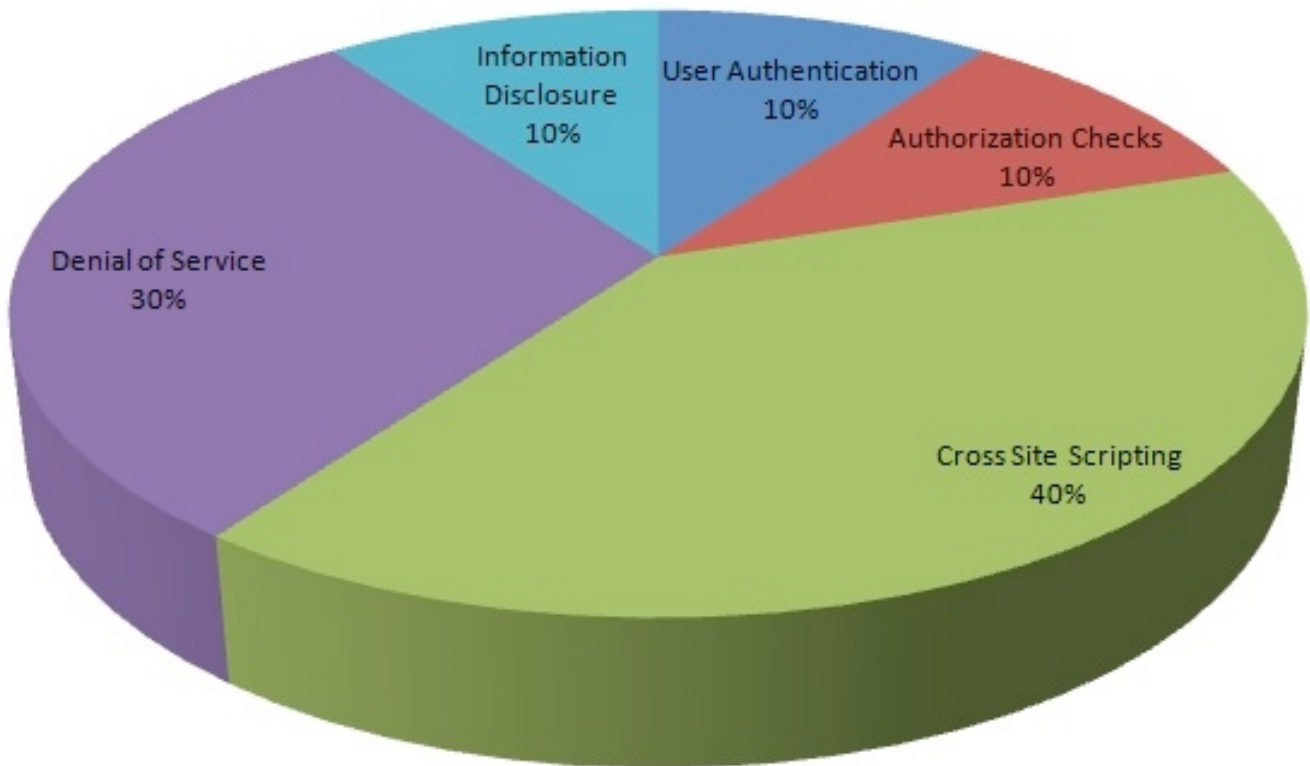
SAP released over 570 Security Notes between January and September 2012. This translates to an average of 60 notes per month. Against these numbers, October appears to be an outlier: there were only ten Security Notes issued by SAP in the month. However, this is likely to be an anomaly. Normal service seems to have resumed in November with over 30 Security Notes released mid-way through the month.

The most critical Note released in October relates to a program error in the server core of the NetWeaver Application Server Java (AS Java). AS Java provides the runtime environment for Java programs based on the J2EE standard. Note 1720677 deals with a vulnerability in AS Java that provides access to protected resources without authentication.

Note 1678387 addresses a Denial-of-Service (DoS) vulnerability that could render the AS Java unavailable. The vulnerability affects the J2EE web container known as servlet_jsp. The container specifies the URL mapping and runtime procedures for Java servlets including rules for security. Communication and transportation services for the web container are handled by the HTTP Provider Service which parses and dispatches requests to the J2EE modules before returning responses to clients. The vulnerability relates to the maximum number of parameters that can be processed for each request. The default is between 1000 - 5000, depending upon the release. Attackers can provoke a DoS through HTTP requests with a higher number of parameters than those accepted by the servlet_jsp. This can cause resource exhaustion and the eventual shutdown of AS Java resources. Customers should update to the latest version of AS Java or apply the relevant SP patch listed in the Note. They should also increase the default value of the MaxParameterCount to higher than 5000 but below 10000.

SAP Security Notes

October 2012



SAP Security Notes by Vulnerability Type

Customers should also closely examine Note 1661336. This addresses an information disclosure vulnerability in the Java Message Service (JMS) Adapter used by Process Integration (PI), the middleware powering SAP system landscapes. Adaptors are used by the PI Integration Engine to process XML messages, Intermediate Documents (IDocs) and Remote Function Calls (RFC). It is also used by the Partner Connectivity Kit, a Java application used to configure message exchange between partners. Note 1661336 patches a vulnerability in the JMS Adapter that could enable attackers to compromise passwords used by the adapter.

Appendix: SAP Security Notes, October 2012

PRIORITY	NOTE	AREA	DESCRIPTION
1	1720677	BC-JAS-SEC	User Guest granted privileges of a real user
2	1772647	CRM-ANA-PS	Update 1 to security note 1610237
2	1773160	BC-FES-ITS	Update 1 to security note 1669031
2	1658025	BC-ABA-SC	Update 1 to security note 1687910
2	1661336	BC-XI-CON-JMS	Potential information disclosure relating to passwords
2	1678387	BC-JAS-WEB	Potential denial of service in AS Java Web container
2	1683929	PT-RC-UI-XS	Unauthorized modification of stored content in PT-RC-UI-XS
2	1724516	BC-CTS-SDM	Multiple security vulnerabilities in SDM
2	1740802	GRC-SPM-SR	Unauthorized modification of displayed content in SuPM 2.0
3	1769046	BC-SEC-USR-ADM	Update 1 to security note 1661157

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

© Copyright Layer Seven Security 2012 - All rights reserved.

No portion of this document may be reproduced in whole or in part without the prior written permission of Layer Seven Security.

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.

This publication contains references to the products of SAP AG. SAP, R/3, xApps, xApp, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius and other Business Objects products and services mentioned herein are trademarks or registered trademarks of Business Objects in the United States and/or other countries.

SAP AG is neither the author nor the publisher of this publication and is not responsible for its content, and SAP Group shall not be liable for errors or omissions with respect to the materials.