Layer Seven Security

ADVISORY

SAP Security Notes

March 2013

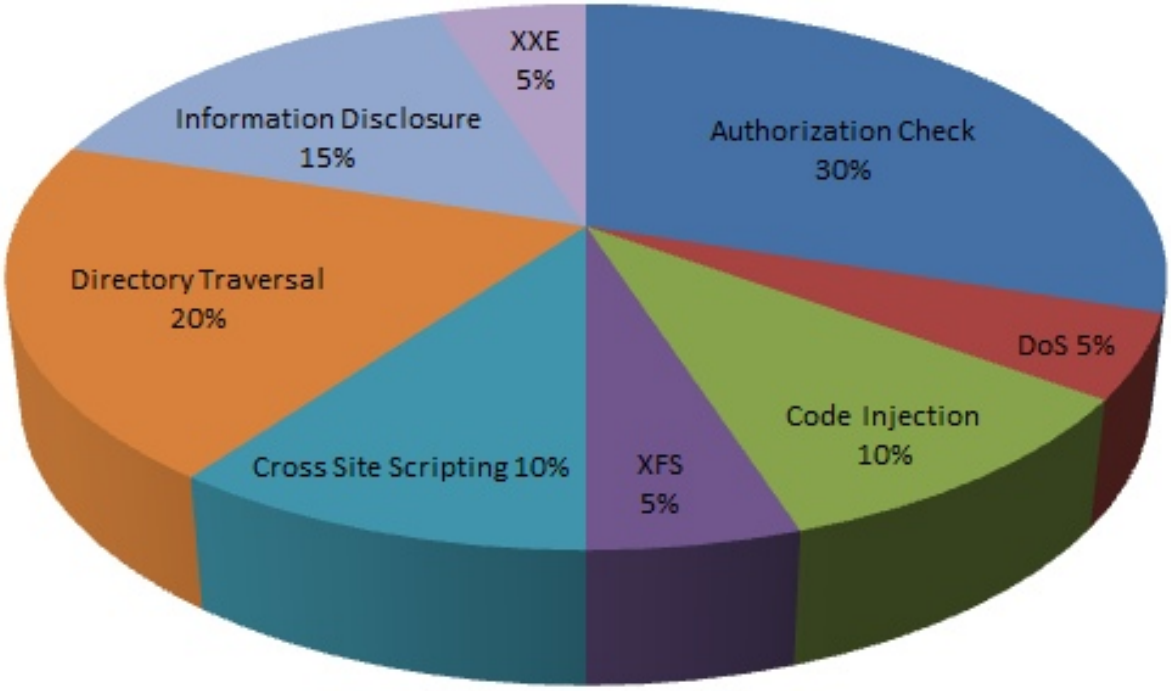
SAP Security Notes

March 2013

The most notable Security Note released in March related to an XML External Entity (XXE) Processing vulnerability in the SAP Software Lifecycle Manager (SLM). SLM is a component of SAP NetWeaver used to design and manage SAP landscapes. It integrates directly with the System Landscape Directory (SLD) which stores information on installed SAP and non-SAP software in landscapes, as well as dependencies, interfaces and other logical connections. It also stores information for business systems managed through SAP Process Integration (PI). Therefore, SLM is a key module of NetWeaver installations and provides visibility to all connected systems in SAP system landscapes.

XXE attacks target vulnerabilities in parsers used to read strings in XML documents and convert information in XML files to DOM objects which are then made available to applications through programming languages such as JavaScript. Malicious system identifiers such as URLs can be accessed by parsers when processing external entities in XML documents. This can enable attackers to access sensitive files and other resources. These resources can be rendered unavailable, provoking a denial of service. Attackers can also use XXE to execute arbitrary code, open TCP connections, or access other systems if compromised applications are configured as trusted systems in internal networks.

Java XML parsers are especially vulnerable to such attacks since XXE is often enabled by default. This can be resolved by configuring parsers to access only local and static Document Type Declarations (DTD) rather than those declared in XML documents. The XXE vulnerability in SLM should be addressed through the application of the appropriate patch level for NetWeaver releases 7.30, 7.31 and 7.40. For further information, refer to Security Note 1820894.



SAP Security Notes by Vulnerability Type

Note 1784894 contended with a reflected cross-site scripting vulnerability (XSS) in the deployment component of the Java Application Server (AS). Reflected XSS is a common vulnerability effecting AS Java components, but is less threatening than persistent or stored XSS which can alter content rendered to all users of an application server through the injection of malicious scripts. In this case, the root cause of the vulnerability was insufficient encoding of user input parameters by a specific Java servlet that manages client requests to certain SAP services. The impact could include the theft of user credentials leading to unauthorized access to SAP systems, changes to underlying data or the compromise of confidential, restricted information. Along with input validation, output encoding is one of the most effective methods for combating XSS vulnerabilities.

Note 1778949 dealt with a crucial vulnerability in the Integration Server of SAP PI. PI supports linkages between internal and external systems through XML and other protocols. The Integration Server lies at the core of PI, providing the runtime environment for cross-system exchange. The Note patched an information disclosure vulnerability in the Server that could be exploited to obtain information such as user passwords.

Note 1779092 carried one of the highest CVSS base scores for all patches released in March (7.8 out of 10). It released a correction for a directory traversal vulnerability in a component of the Enterprise Portal Infrastructure caused by a programming error that failed to validate paths for file references on remote servers. The vulnerability could lead to unauthorized disclosure of information in files located on SAP servers.

Appendix: SAP Security Notes, March 2013

PRIORITY	NOTE	AREA	DESCRIPTION
2	1820894	BC-UPG-SLM	Security fix for SLM treating XXE vulnerability
2	1813734	CA-TDM-BPL	Missing authorization check in DMIS_EXT
2	1808402	BC-SRV-BRF	Missing authorization check in BC-SRV-BRF
2	1795103	CA-EUR	Code injection vulnerability in component DMIS
2	1789823	BC-BMT-WFM	Missing authorization check in BC-BMT-WFM
2	1786822	BW-BEX-OT-OLAP	Code injection vulnerability in BW-BEX-OT-OLAP
2	1784894	BC-JAS-DPL	Unauthorized modification of displayed content in a NWA app
2	1778949	BC-XI-IS	Potential disclosure of information about PI
2	1771567	SV-SMG-CDM	Missing Authorization Check in CDMC (component ST-PI)
2	1741793	BC-CST-DP	Potential remote termination of running work processes
2	1715734	BC-JAS-TRH	Missing authorization check in dbpool administration
2	1706335	BC-FES-BUS-HTM	Unauthorized modification of displayed content in NWBC
2	1839511	BC-JAS-SEC	Update 2 to security note 1651004
3	1807196	CA-CL	CA-CL: Directory traversal vulnerability
3	1806435	BW-EI-RTR	Missing authorization check in BW-EI-RTR
3	1789611	BC-MOB-MI	Potential information disclosure relating to BC-MOB-MI
3	1779092	EP-PIN-PRT-WS	Directory traversal in the portal SoapApplication
3	1768943	PY-IT	Potential directory traversal in PY-IT
3	1760776	PY-NL	Directory traversal in PY-NL-RP, PA-PA-NL and PA-PF-NL
4	1685106	BC-JAS-ADM-LOG	Potential information disclosure related to SAP AS Java

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