ADVISORY

Layer Seven Security

SAP Security Notes

February 2015

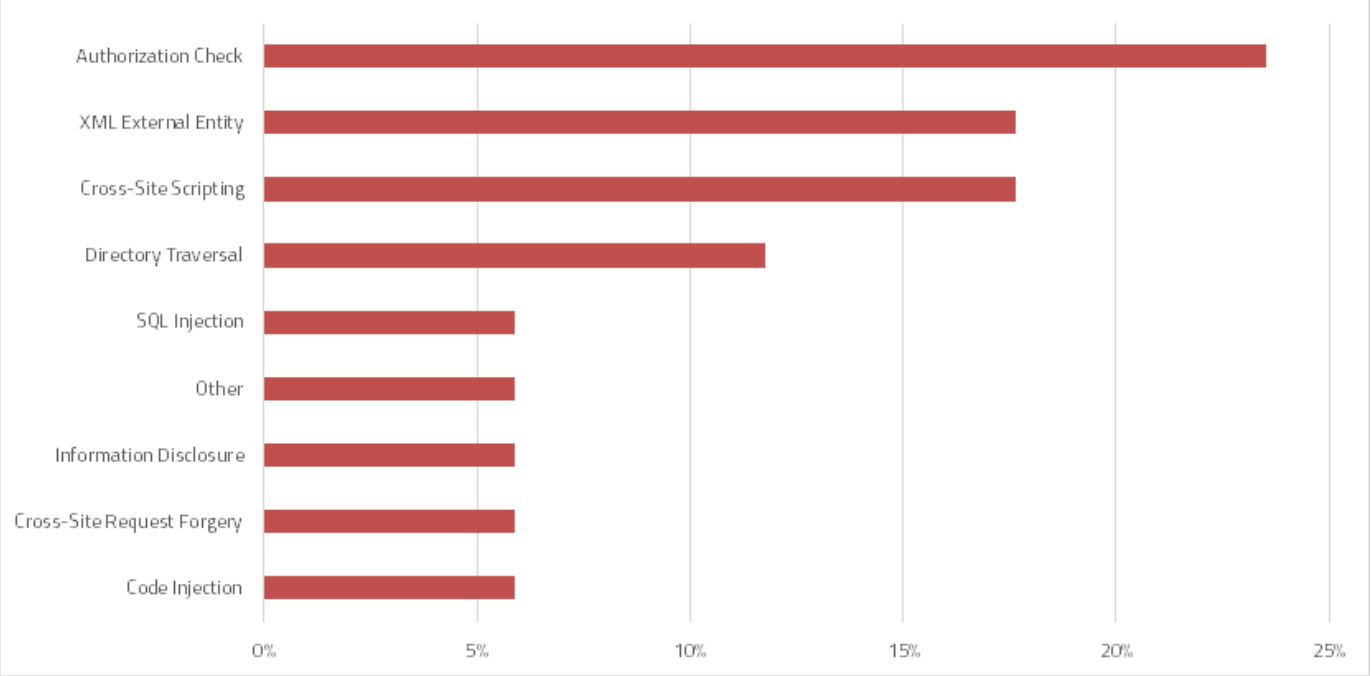
SAP Security Notes

February 2015

SAP released several patches in February for dangerous XML External Entity (XXE) vulnerabilities impacting components of the Enterprise Portal and the Mobile Platform. XXE vulnerabilities often exploit the local administrative privileges granted to XML parsers. They arise when XML processors do not adequately parse XML input. This can enable attackers to change external entity values with malicious data or alter URLs to point to external servers. The latter can be abused to download and install programs to support more destructive secondary attacks. Attackers can also exploit XXE vulnerabilities to access or corrupt sensitive files and provoke a denial of service. XXE attacks can be prevented by configuring XML processors to support only static document type declaration (DTD) rather than declared DTD in XML documents. Given the severity of XXE attacks, customers with SAP Portals or Mobile Platforms should implement the correction instructions included in Notes 2125358, 2098608 and 2093966.

Note 2063369 patches a buffer overflow vulnerability that could enable attackers to inject malicious code into the working memory of profile maintenance. The vulnerability could lead to the complete compromise of the tool commonly used by security administrators to manage role and authorization data in SAP systems. The correction requires the implementation of the relevant support package for each system referenced in the Note. This will update the kernel-level dis+work.exe program that manages front-end communication and work processes for each instance.

Note 2023388 deals with an information disclosure vulnerability that could lead



SAP Security Notes by Vulnerability Type

attackers to discover passwords used for Process Integration in log entries accessible using the log viewer. The log viewer can be accessed through the NetWeaver Administrator and provides access to trace and error messages generated across entire SAP system landscapes.

Note 2109818 applies changes to the log writing function to prevent attackers from generating fictitious log entries in HANA XS, an application server integrated into the HANA platform. Although the vulnerability addressed by the Note doesn't enable attackers to read or change genuine log entries, it can be exploited to obstruct forensic analysis and investigations.

Lastly, Note 2030997 introduces switchable authorization checks for RFC-enabled function modules in Accounts Payable FI-AP, a core component of the Financials module in SAP ERP. Switchable authorization checks enable customers to improve security for critical RFMs by introducing an additional check beyond the standard check for the S_RFC authorization object. The specific function modules impacted by Note 2030997 are FI_AP_VENDOR_BAPI and BAPI_CREDITOR_FIND. These are business application programming interfaces implemented as function modules that provide access to vendor and creditor data.

Appendix: SAP Security Notes, February 2015

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2111541	BW-WHM-DBA	Update 1 to Security Note 1965819
HIGH	2109818	HAN-AS-XS	Potential log injection vulnerability in SAP HANA Extended Application Services
HIGH	2125358	MOB-ONP	SAP Mobile Platform XXE vulnarability
HIGH	2115610	CA-TDM	Missing authorization check in DMIS_BSC and DMIS_CNT
HIGH	2114316	MOB-ONP-COR	Unauthorized use of application functions in SMP 3.0
HIGH	2099500	BC-JAS-SEC	Missing Authorization Check in SPNego Wizard
HIGH	2093966	EP-PIN-IVS-UPL	XML External Entity vulnerability in SAP XML Parser
HIGH	2073693	BI-BIP-INV	Unauthorized modification of displayed content in BI-BIP-INV
HIGH	2063369	BC-CCM-CNF-PFL	Potential remote code execution in profile maintenance
HIGH	2023388	BC-XI-CON-AFW-DC	Potential information disclosure relating to password
MEDIUM	1944155	CO-PA	Missing authority check in Report RKEDELE1
MEDIUM	1823920	CA-DMS	Directory traversal in CA-DMS
MEDIUM	2033772	MOB-AFA	SAP Afaria Client XeService.exe unquoted path vulnerability
MEDIUM	2098608	EP-PIN-IVS-UPL	XML External Entity vulnerability in SAP XML Parser
MEDIUM	2095236	BI-RA-WBI-FE-HTM	Unauthorized modification of displayed content in Web interface of Web Intelligence document
MEDIUM	1874288	EP-PIN-RTM	Unauthorized modification of displayed content in RTMF
MEDIUM	2030997	FI-AP-AP	Switchable authorization checks for RFC in FI-AP-AP

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