


Layer Seven Security

SAP Security Notes

May 2014



SAP released two Hot News patches in May. The first deals with the well-known Heartbleed vulnerability in OpenSSL software packaged within Document Presentment for SAP. For further information on Heartbleed, please refer to last month's Advisory issued by Layer Seven Security, as well as <http://heartbleed.com> and http://www.openssl.org/news/secadv_20140407.txt.

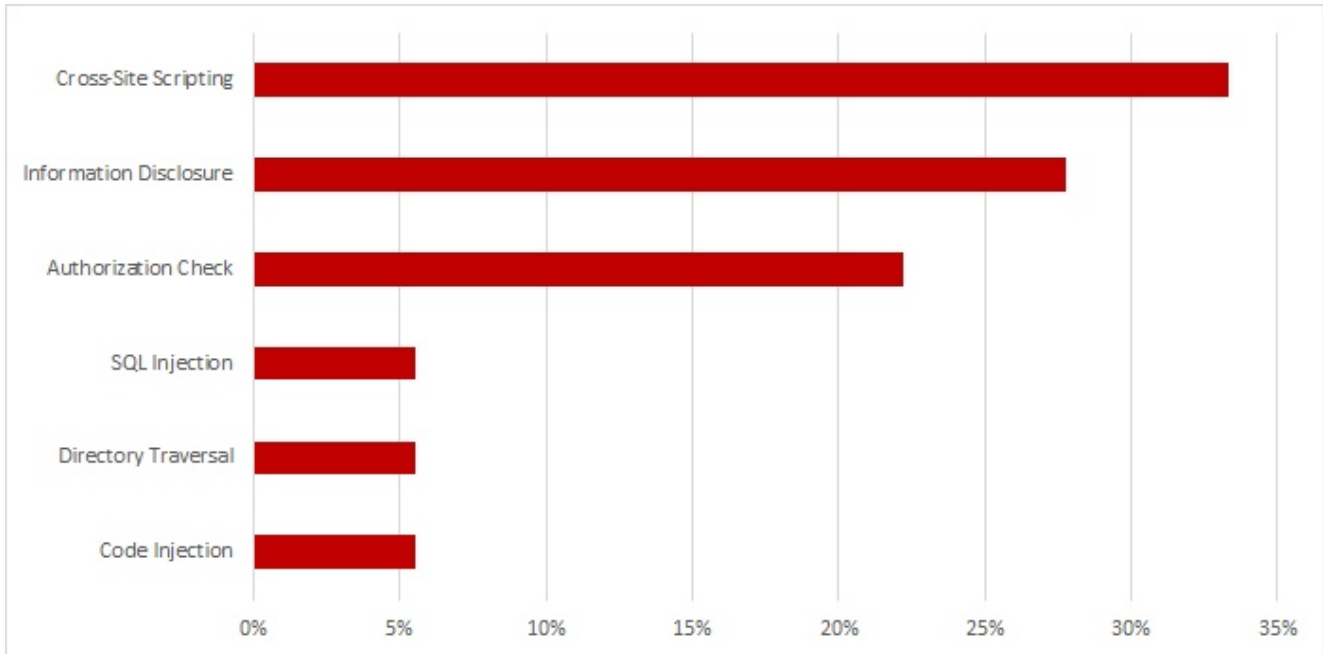
Document Presentment for SAP is a third-party solution developed by OpenText that supports document creation, changes and distribution in SAP environments. Note 2018190 includes separate patches for versions 5.6 and 5.6.1 of the solution. SAP customers impacted by the vulnerability are also advised to revoke compromised certificates and keys, reissue and distribute new certificates and keys, and change compromised passwords.

The second Hot News patch deals with a code injection vulnerability in all versions of SAP Online Banking using Apache Struts 2.0.0 - 2.3.16.1, an open-source framework for creating web-based Java applications. The ParametersInterceptor in effected versions of Apache Struts does not properly restrict access to the getClass method. This enables remote attackers to manipulate the ClassLoader and execute arbitrary code via specially-crafted requests. Note 2015882 includes patches to upgrade Apache Struts in SAP Online Banking to 2.3.16.2 which include fixes for the ParametersInterceptor.

There were multiple high-priority Notes released in May for various components of SAP Customer Relationship Management (CRM) including Communications, E-Commerce, Marketing, and Trade Promotions. Notes 1979438, 1977754, 2000476, 1997788, 1990115 and 1674849 deal with missing authorization checks, cross-site scripting and information disclosure vulnerabilities that could lead to the theft of user credentials and other

SAP Security Notes

May 2014



SAP Security Notes by Vulnerability Type

sensitive data and unauthorized access to SAP resources and systems.

Finally, Note 1997455 delivers a new version of the role SAP_BC_USR_CUA_CENTRAL to resolve a vulnerability in Central User Administration (CUA) that could enable attackers to read information in all central CUA system tables. CUA provides a platform for centralized user management in SAP landscapes.

Appendix: SAP Security Notes, May 2014

| PRIORITY | NOTE | AREA | DESCRIPTION |
|----------|---------|-----------------|--|
| HOT NEWS | 2018190 | XX-PART-OPT-DPR | OpenSSL vulnerability (Heartbleed bug) in SAP Document Presentment by OpenText 5.6 / 5.6.1 |
| HOT NEWS | 2015882 | MOB-MCO-EBK | Apache Struts 2 Vulnerability in SAP Online Banking |
| HIGH | 1889999 | BC-DB-LCA | Missing authorization check in LCAPPS DP |
| HIGH | 1984057 | BC-SRV-KPR | Update #1 to Security Note 1635004 |
| HIGH | 1979438 | CRM-ISA-BBS | Unauthorized modification of displayed content in CRM-ISA-BBS |
| HIGH | 1977754 | CRM-ISA | Potential information disclosure relating to CRM-ISA/CRM-ISE |
| HIGH | 1977547 | BC-UPG-TLS-TLA | Update 1 to Security Note 1584573 |
| HIGH | 1966995 | BC-FES-BUS | Potential information disclosure relating to WebDynpro Application |
| HIGH | 2000476 | CRM-MKT-MPL | Missing authorization check in CRM-MKT-MPL |
| HIGH | 1997788 | CRM-MKT-MPL-TPM | Missing authorization check in CRM-MKT-MPL-TPM |
| HIGH | 1997455 | BC-SEC-USR-ADM | Potential information disclosure in BC-SEC-USR-ADM |
| HIGH | 1990115 | CRM-ISA | Unauthorized modification of displayed content in CRM-ISA |
| HIGH | 1674849 | CRM-IC-CHA | Unauthorized modification in BSP application in CRM-IC-CHA |
| MEDIUM | 1621071 | IS-R-RA | Unauthorized modification of displayed content in IS-R-RA |
| MEDIUM | 1808003 | BC-CST | Potential information disclosure relating to BC-CST |
| MEDIUM | 1941796 | EP-PIN-AI | Unauthorized modification of stored content in Application Integration Transaction JavaGui component |
| MEDIUM | 1915920 | FS-RI-AC-RM | Missing authorization check in FS-RI |
| MEDIUM | 2009696 | HAN-AS-XS | Unauthorized modification of displayed content in SHINE |



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



© Copyright Layer Seven Security 2014 - 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.