




LAYER SEVEN SECURITY

# SAP Security Notes

December 2018

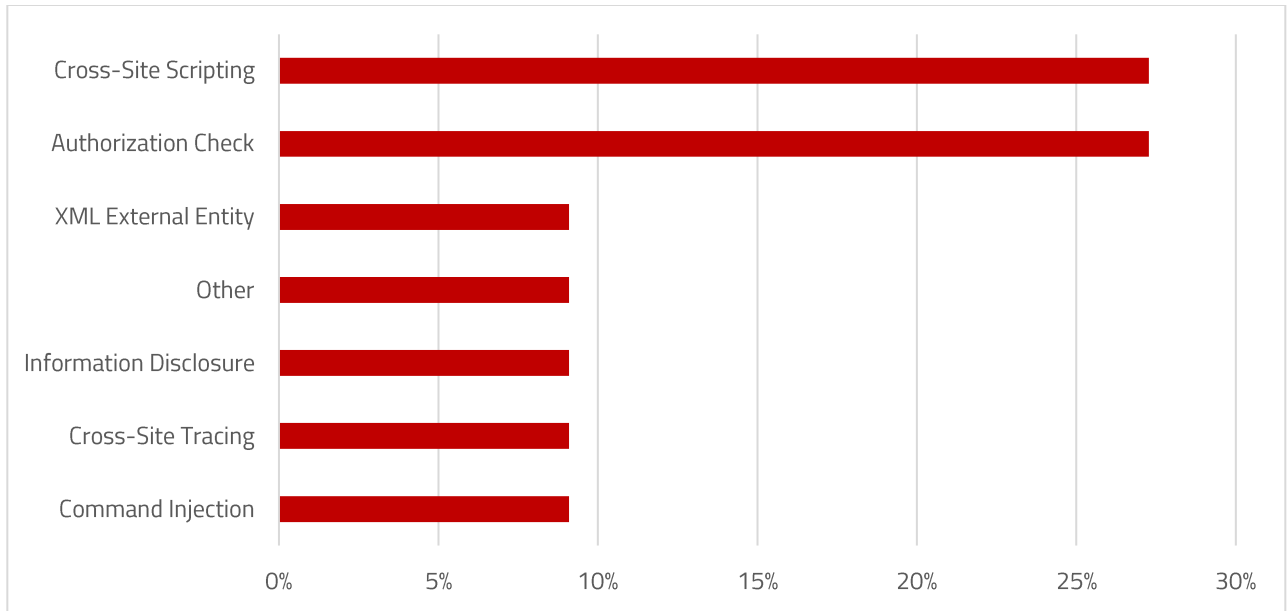


Hot News Note 2711425 patches a critical Cross-Site Scripting (XSS) vulnerability in SAP Hybris Commerce storefronts. The vulnerability could be exploited by attackers to modify web content and compromise user-related authentication data. It affects versions 6.2 through 6.7 and 18.08 of SAP Hybris Commerce, including all but the latest patch releases. The vulnerability carries a CVSS v3.0 base score of 9.3/10 and scores particularly high in terms of impact to confidentiality and integrity. The related exploit is relatively non-complex and does not require any privileges in the target system. In addition to applying the automated updates referenced in Note 2711425, manual steps may be required to remove the vulnerability in cases where custom HTTP headers are used for caching, SAP Hybris Commerce is positioned behind a HTTP reverse proxy or load balancer, or the system is used in conjunction with a content delivery network (CDN).

Note 2642680 deals with a high-risk XML External Entity (XXE) vulnerability in SAP NetWeaver Application Server Java (AS Java) caused by missing validation for XML documents received from untrusted sources. The vulnerability could lead to the compromise of the SAP file system or enable attackers to provoke a denial of service.

## SAP Security Notes

December 2018



## SAP Security Notes by Vulnerability Type

Note 2658279 patches an insufficient authorization check impacting the AS Java keystore service.

Note 2698996 removes a missing authorization check in SAP Customizing Tools. The note introduces a check for object S\_RFC\_ADM to prevent an escalation of privileges.

## Appendix: SAP Security Notes, December 2018

| PRIORITY | NOTE    | AREA            | DESCRIPTION   |
|----------|---------|-----------------|---|
| HOT NEWS | 2711425 | CEC-COM-CPS-CKP | [CVE-2018-2505] Cross-Site Scripting (XSS) vulnerability in SAP Hybris Commerce storefronts |
| HIGH     | 2642680 | BC-JAS-SEC-LGN  | [CVE-2018-2492] Missing XML Validation in SAP NetWeaver AS Java                             |
| HIGH     | 2698996 | BC-CUS-TOL-CST  | [CVE-2018-2494] Missing Authorization check in SAP Customizing Tools                        |
| HIGH     | 2658279 | BC-JAS-SEC      | [CVE-2018-2503] Wrong default authorizations in AS Java keystore service                    |
| MEDIUM   | 1610734 | AP-MD-BP        | Missing authorization check in Application Platform MD-BP                                   |
| MEDIUM   | 2561202 | BI-RA-WBI-BE-DP | Command Injection through Web Intelligence Report or DataProvider export                    |
| MEDIUM   | 2680492 | SBO-CRO-SEC     | [CVE-2018-2502] Insecure HTTP Method Enabled in SAP Business One Service Layer              |
| MEDIUM   | 2718993 | BC-JAS-WEB      | [CVE-2018-2504] Cross-Site Scripting using host header in SAP NetWeaver AS Java             |
| MEDIUM   | 2707024 | MOB-AFA-DEV     | [CVE-2018-2500] Information Disclosure in Mobile Secure Android client                      |
| MEDIUM   | 2705204 | CEC-MKT-MEM     | [CVE-2018-2486] Cross-Site Scripting (XSS) vulnerability in SAP Marketing Content Studio    |
| LOW      | 2704878 | HAN-DB-SEC      | [CVE-2018-2497] Event not logged in SAP HANA database audit log                             |



**LAYER SEVEN SECURITY**

Layer Seven Security secure, patch and monitor SAP systems against cyber threats using SAP Solution Manager. Layer Seven's innovative and patent-pending Cybersecurity Extension for Solution Manager extends the capabilities of Solution Manager for advanced vulnerability management, threat detection and incident response.

**Address**

99 Hudson Street  
5th Floor  
New York, NY 10013  
United States

**Web**

[www.layersevensecurity.com](http://www.layersevensecurity.com)

**Email**

[info@layersevensecurity.com](mailto:info@layersevensecurity.com)

**Telephone**

1-647-964-7370



© Copyright Layer Seven Security 2018 - 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.