LAYER SEVEN SECURITY

ADVISORY

# SAP Security Notes

October 2018

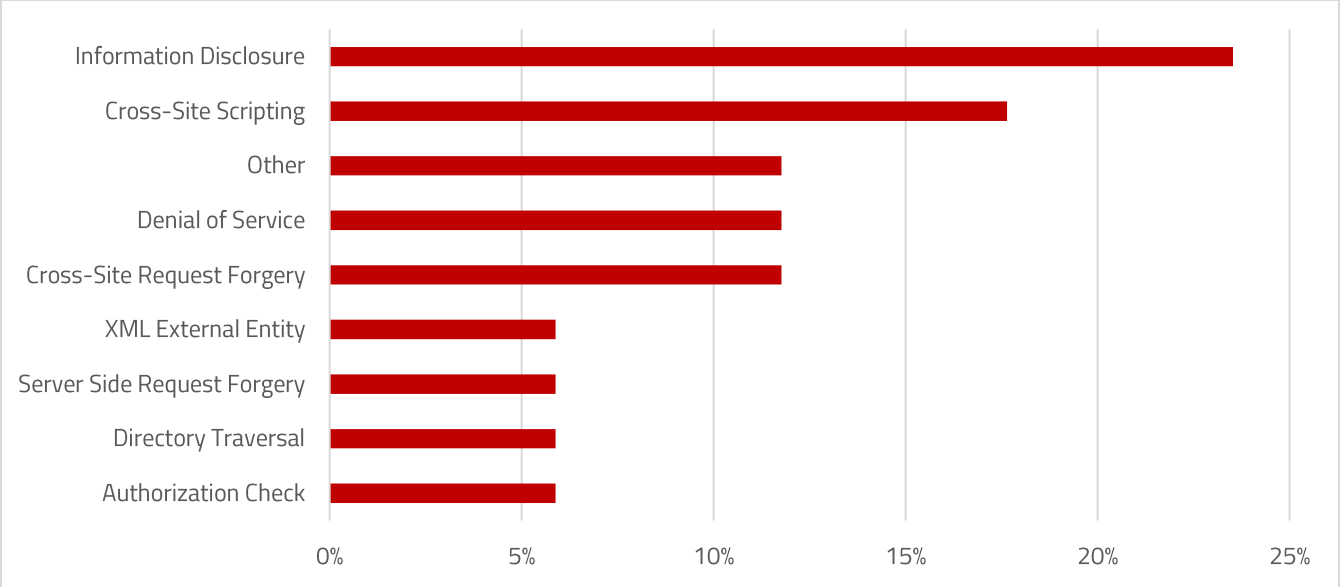
# SAP Security Notes

October 2018

Hot News note 2654905 patches a high risk information disclosure vulnerability in the SAP BusinessObjects BI Suite. The execution of specific CMS queries on the Central Management Server could bypass authorization checks and lead to the leakage of sensitive data. The vulnerability scores 9.8/ 10 based on the Common Vulnerability Scoring System v3 (CVSS). Patches for BI 4.1 SP 10-12 and 4.2 SP 4-6 referenced in the Note enable authorization checks for vulnerable CMS queries.

Note 2699726 provides corrections to remove a missing network isolation error in SAP's Open Source project Gardener. Gardener is an API server that provides Kubernetes clusters for several SAP products. SAP is responsible for security updates for Gardener instances and Gardener managed Kubernetes clusters at SAP. Note 2699726 applies only to Gardener stakeholders in the Open Source Community who operate their own Gardener installations. The Note recommends upgrading to Gardener release 0.12.4 or higher in order to prevent admins in shoot clusters from compromising seed clusters or other shoot clusters.

Note 2696962 provides instructions for dealing with a Denial of Service (DoS) vulnerability in the SQLite database engine of SAPFoundation. SQLite is embedded in the SAP Cloud Platform SDK for iOS 2.0 SP02 and 3.0.




## SAP Security Notes by Vulnerability Type

Note 2674215 provides corrections for patching a stack overflow vulnerability that could be exploited by attackers to provoke a denial of service in SAP Plant Connectivity.

# Appendix: SAP Security Notes, October 2018

| PRIORITY | NOTE | AREA | DESCRIPTION |
|---|---|---|---|
| HOT NEWS | 2654905 | BI-BIP-SRV | [CVE-2018-2471] Information Disclosure in SAP BusinessObjects BI Suite |
| HIGH | 2699726 | BC-NEO-K8S | [CVE-2018-2475] Missing network isolation in Gardener |
| HIGH | 2696962 | MOB-SDK-IOS | Denial of Service(DoS) vulnerability in SAPFoundation / database |
| HIGH | 2674215 | MFG-PCO | Denial of service (DOS) in OPC UA applications of SAP Plant Connectivity |
| MEDIUM | 1517831 | PY-NPO | Potential Directory Traversal in SAP HCM Payroll NPO |
| MEDIUM | 2630018 | BI-BIP-CMC | [CVE-2018-2445] Server Side Request Forgery(SSRF) vulnerability in SAP BusinessObjects BI Platform Servers AdminTools |
| MEDIUM | 2684760 | BC-BSP | [CVE-2018-2470] Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver AS ABAP Business Server Pages |
| MEDIUM | 2679789 | BC-SYB-ASE | [CVE-2018-2469] Information Disclosure in SAP Adaptive Server Enterprise |
| MEDIUM | 2678615 | BC-SYB-ASE | [CVE-2018-2468] Information Disclosure in SAP Adaptive Server Enterprise/Backup Server |
| MEDIUM | 2667103 | BI-RA-WBI-FE-HTM | [CVE-2018-2472] Cross-Site Scripting (XSS) vulnerability in SAP Web Intelligence DHTML client |
| MEDIUM | 2623618 | BI-RA-WBI-SDK | [CVE-2018-2467] File Path Disclosure in SAP Business Intelligence Software Development Kit |
| MEDIUM | 2696889 | PA-FIO-LEA | [CVE-2018-2474] Cross-Site Request Forgery (CSRF) vulnerability in SAP Approve Leave Request V2 application |
| MEDIUM | 2688018 | PA-FIO-LEA | [CVE-2018-2474] Cross-Site Request Forgery (CSRF) vulnerability in SAP Approve Leave Request V2 application |
| MEDIUM | 2618337 | EIM-DS-DES | [CVE-2018-2466] Cross-Site Scripting (XSS) vulnerability in SAP Data Services Management Console |
| MEDIUM | 2272676 | BC-WD-CMP-ALV-ABA | Spreadsheet Formula Injection in FPM List UIBB ATS/FPM Tree UIBB/WD ALV |
| MEDIUM | 2275009 | CRM-MW-ADP | Switchable authorization checks for RFC in CRM-MW-ADP |
| MEDIUM | 2665970 | MFG-PCO | Missing XML Validation vulnerability in Plant Connectivity (PCo) |

LAYER SEVEN SECURITY

Layer Seven Security serve customers worldwide to harden, patch and monitor SAP systems against cyber threats using SAP Solution Manager


**Address**

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

**Web**

www.layersevensecurity.com

**Email**

info@layersevensecurity.com

**Telephone**

1-647-964-7370