LAYER SEVEN SECURITY

ADVISORY

SAP Security Notes

July 2018

SAP Security Notes

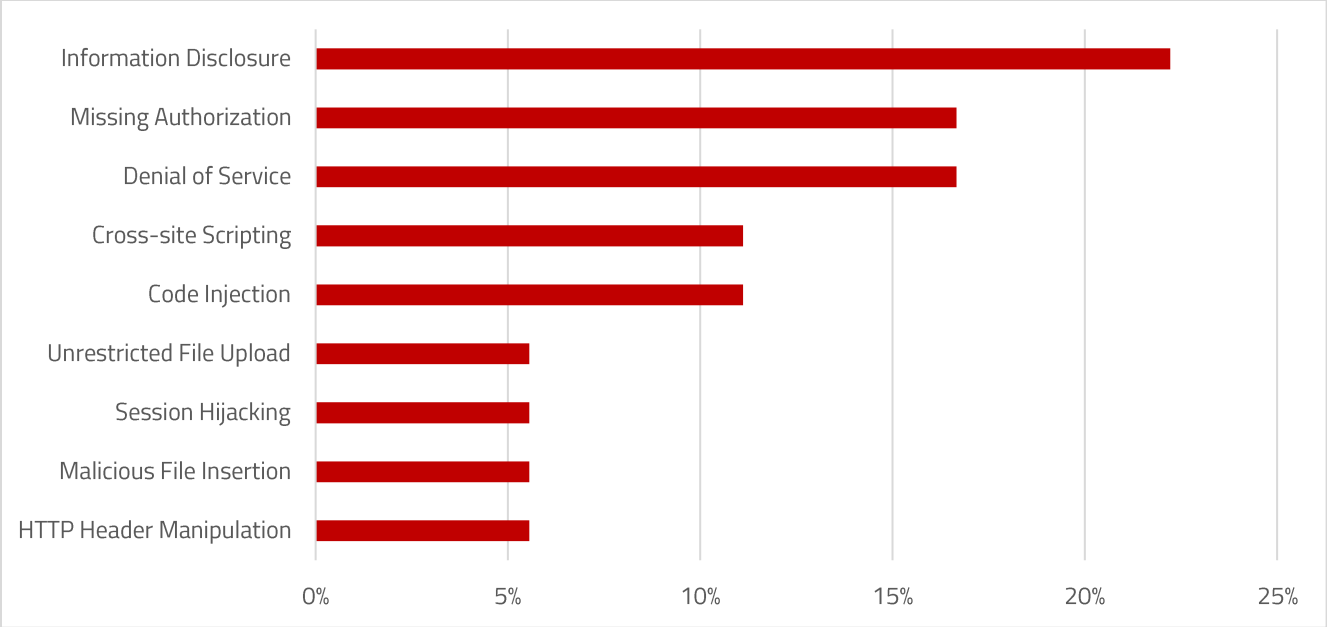
July 2018

Notes 2017041 and 2016974 patch high-risk information disclosure vulnerabilities in SAP Environment, Health & Safety Management (EHSM). The vulnerabilities could be exploited to leak sensitive information stored or processed by the transactional Fiori apps Inspect Safety Controls and Retrieve Safety Information. The apps support the performance and tracking of safety control inspections.

Note 2641674 provides corrections to support virus scanning for OData v2 connections in the SAP Gateway using the SAP Virus Scan Interface (VSI). This will protect against the insertion of untrusted files and malware.

Note 2597913 includes a kernel patch to remove a Denial of Service vulnerability in the SAP Gateway that could enable attackers to provoke resource exhaustion by flooding specific services. The relatively low CVSS score for the note is misleading. Exploitation of the vulnerability requires network-level access only and does not require any privileges in the system. Furthermore, the impact in terms of system availability is high.

Note 2622434 removes passwords in route strings that are forwarded from one SAProuter to another. Route strings define permitted connections, users and services between hosts. The leakage of passwords could lead to targeted attacks against the SAProuter.



SAP Security Notes by Vulnerability Type

Finally, Note 2664767 removes the logging of sensitive data in logs for SAP Dynamic Authorization Management (DAM) by NextLabs. DAM supports attribute or policy-based access control to manage user privileges.

Appendix: SAP Security Notes, July 2018

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2017041	EHS-MGM-RAS	Potential information disclosure relating to Inspect Safety Controls
HIGH	2016974	EHS-MGM-RAS	Potential information disclosure relating to Retrieve Safety Information
MEDIUM	2641674	OPU-GW-COR	Unrestricted File Upload vulnerability in SAP Gateway
MEDIUM	2633366	BC-ABA-XML	Denial of service (DOS) in iXML Toolset of SAP Kernel
MEDIUM	2622434	BC-CST-NI	Information disclosure relating to password in SAProuter
MEDIUM	2664767	XX-PART-NXL	[CVE-2018-2440] Sensitive Information Exposure in SAP Dynamic Authorization Management by NextLabs
MEDIUM	2523290	BI-BIP-INV	[CVE-2018-2432] Header Manipulation vulnerability in BI LaunchPad and CMC
MEDIUM	2644227	BC-FES-IGS	[CVE-2018-2437] Unauthorized Command execution in SAP Internet Graphics Server (IGS)
MEDIUM	2644238	BC-FES-IGS	[CVE-2018-2438] Denial of service (DOS) in SAP Internet Graphics Server (IGS)
MEDIUM	2644147	BC-FES-IGS	[CVE-2018-2439] Code Injection vulnerability in SAP Internet Graphics Server (IGS)
MEDIUM	2643126	EP-PIN-PRT	[CVE-2018-2435] Cross-site Scripting (XSS) in SAP NetWeaver Enterprise Portal
MEDIUM	2624762	BI-RA-CR-VW	[CVE-2018-2431] Cross-Site Scripting (XSS) vulnerability in SAP CrystalReports
MEDIUM	2620738	BI-RA-CR-VW	[CVE-2018-2427] Code Injection vulnerability in SAP CrystalReports
MEDIUM	2652578	IS-R-PUR-RP	[CVE-2018-2436] Missing Authorization check in Function Module WRCK_STORE_LOESCH_KONSISTENZ
MEDIUM	2597913	BC-CST-GW	[CVE-2018-2433] Denial of Service (DOS) in SAP Gateway
MEDIUM	2519562	XX-CSC-AR-LO	Missing Authorization check in XX-CSC-AR-LO
LOW	2307916	CRM-BF-PC	Missing Authorization check in component CRM-BF-PC
LOW	2180849	XX-PART-ADB-IFD	Logout Button missing in Config UI of Adobe Document Services on HCP

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

© Copyright Layer Seven Security 2018 - All rights reserved.