Layer Seven Security

ADVISORY

SAP Security Notes

August 2017

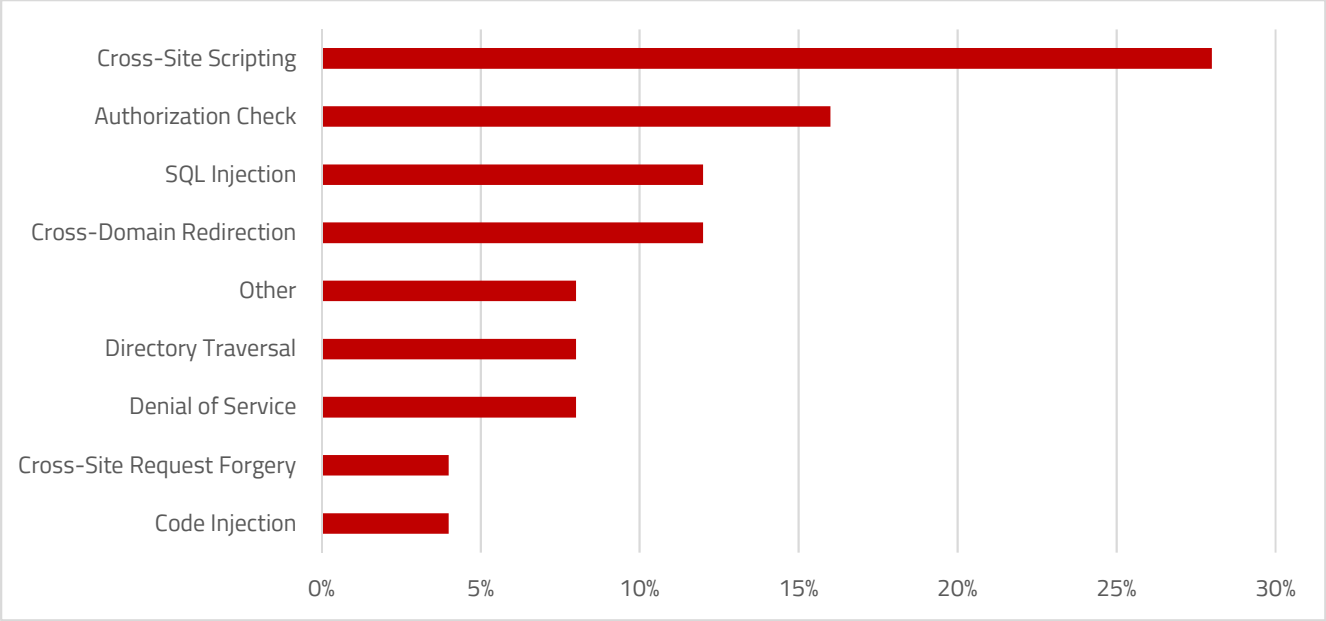
SAP Security Notes

August 2017

Note 2381071 patches a critical cross-site Ajax vulnerability in the Prototype JS library of BusinessObjects. Ajax is a method often used by JavaScripts to exchange data between servers and clients to update parts of web pages without refreshing or reloading entire pages. This minimizes network bandwidth usage and also improves response times through rapid operations. Ajax is an acronym for Asynchronous JavaScript and XML since it's applied via XmlHttpRequest objects that interact dynamically with servers using JavaScript. XMLHttpRequest objects call server-side objects like pages and web services.

Browsers commonly apply a same-origin policy that prevent pages from accessing external resources that have a different scheme, hostname or port than existing pages. However, same-origin policies can be bypassed using procedures such as cross-origin resource sharing. This could be exploited to transmit or load sensitive data to/ from malicious servers. The cross-site Ajax request vulnerability addressed by Note 2381071 applies to versions 4.0 – 4.2 of BusinessObjects. Corrections are included in the patch levels for each relevant support package.

Note 2486657 deals with a high-risk directory traversal vulnerability in the NetWeaver AS Java Web Container. The Web Container is a component of the J2EE Engine and provides the runtime environment for Java applications including servlets and BSPs.



SAP Security Notes by Vulnerability Type

It receives HTTP requests from clients via the AS Java dispatcher. The requests are processed by applications in the Web Container to access business objects in the EJB Container. Note 2486657 improves input validation for file paths to prevent applications using the Servlet API exposing resources in parent directories or other directories outside the application context.

Other important notes include Notes 2376081, 2423540, 2524134 and 2280932 that patch a code injection vulnerability impacting iviews in Visual Composer, a URL redirection vulnerability in the SAP NetWeaver Logon Application, and a missing authorization check in the Security Provider Service.

Appendix: SAP Security Notes, August 2017 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HIGH	2381071	BI-BIP-BIW	Cross-Site AJAX Requests vulnerability in SAP BusinessObjects
HIGH	2486657	BC-JAS-WEB	Directory Traversal vulnerability in SAP NetWeaver AS Java Web Container
HIGH	2376081	EP-VC-04S	Code Injection vulnerability in Visual Composer 04s iviews
MEDIUM	2524134	BC-JAS-SEC	Update 1 to 2423540: URL Redirection Vulnerability in SAP NetWeaver Logon Application
MEDIUM	2423540	BC-JAS-SEC	URL Redirection Vulnerability in SAP NetWeaver Logon Application
MEDIUM	2497027	XX-CSC-BR-NFE	Missing Authorization check in XX-CSC-BR-NFE
MEDIUM	2132282	BC-BMT-WFM-WEB	Potential denial of service in BC-BMT-WFM-WEB
MEDIUM	2189781	BC-FES-BUS-HTM	Unauthorized modification of displayed content in NWBC for HTML
MEDIUM	2280932	BC-JAS-SEC-LGN	Missing Authorization Check in Security Provider Service
MEDIUM	2271802	CRM-MKT-EAL	Switchable authorization checks for RFC in External List Management (CRM-MKT-EAL)
MEDIUM	2453642	BW-SYS-DB-DB2	SQL Injection vulnerability in SAP NetWeaver
MEDIUM	2450979	CA-WUI-UI	SQL Injection vulnerability in SAP CRM WebClient User Interface
MEDIUM	2493099	SRM-LA	Multiple Security Vulnerabilities in SAP SRM Live Auction Application
MEDIUM	2499109	BC-JAS-SEC-CPG	Collisions during UUID generation in SAP NetWeaver Java Server
MEDIUM	2392719	XX-PART-ADB-IFM	Potential Denial of Service vulnerability in Adobe Document Services
MEDIUM	2494184	BC-SYB-SQA	Cross-Site Request Forgery (CSRF) vulnerability in multiple SAP Sybase products
MEDIUM	2481262	CRM-BF-CFG	Cross-Site Scripting (XSS) vulnerability in SAP CRM IPC Pricing
MEDIUM	2428512	BI-RA-WBI-FE-HTM	Server-Side Request Forgery (SSRF) vulnerability in Web Intelligence BI Launchpad
MEDIUM	2425744	CA-WUI-UI	Cross-Site Scripting (XSS) vulnerability in SAP CRM WebClient UI
MEDIUM	2417020	BC-FES-BUS-HTM	Cross-Site Scripting (XSS) vulnerability in SAP NetWeaver Business Client for HTML

Appendix: SAP Security Notes, August 2017 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
MEDIUM	2393021	BC-WD-CLT-FLX	Adobe SDK XSS vulnerability - Flex
MEDIUM	1786732	XX-CSC-BR	Directory traversal in J1BA
LOW	2491763	GRC-SAC-ARA	SQL Injection vulnerability in GRC Access Controls
LOW	2463354	BC-DWB-TOO-CLA	Missing Authorization check in the ABAP Workbench tools
LOW	2394536	EP-PIN-WPC-WCM	URL Redirection vulnerability in SAP NetWeaver K.M. Web Page Composer

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

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.