Layer Seven Security

ADVISORY

SAP Security Notes

April 2014

SAP Security Notes

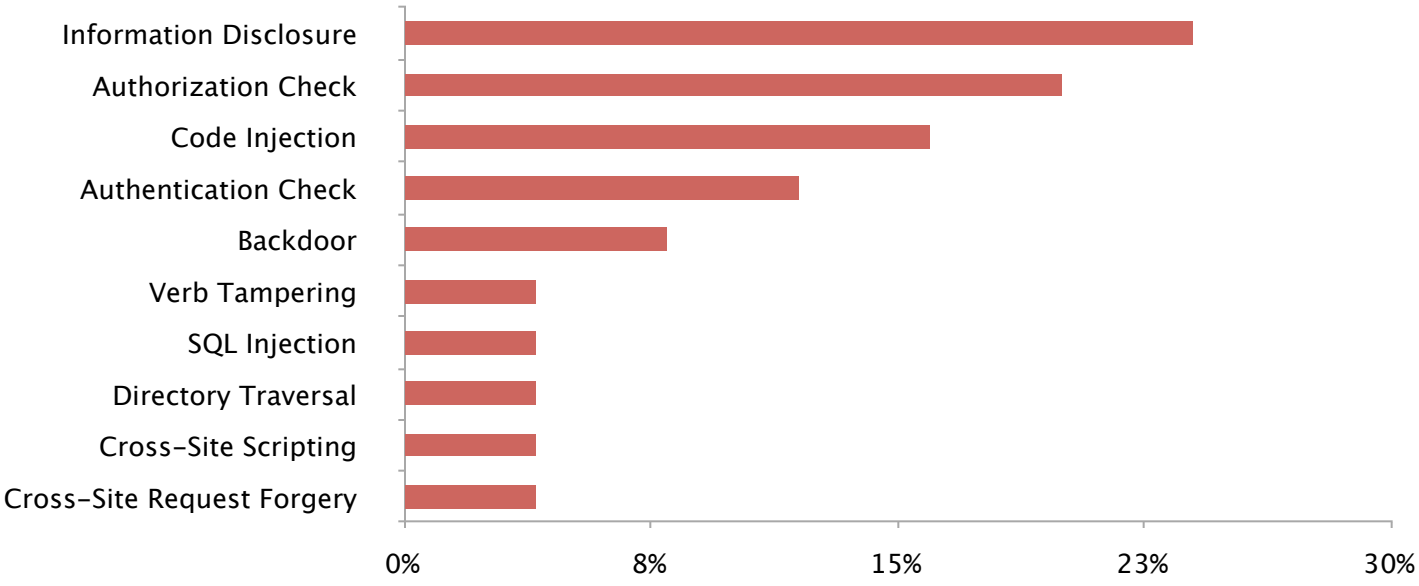
April 2014

On April 11, SAP issued a general statement on the impact of the Heartbleed vulnerability on SAP products. According to the statement, SAP is currently investigating the full extent of the impact but early indications are that SAP NetWeaver and SAP HANA are not impacted. Cryptographic libraries in both platforms do not use OpenSSL.

OpenSSL is an open-source cryptographic library that implements authentication, encryption and other security functions in accordance with the SSL/ TLS protocol. It is used by approximately 1 in 7 of the world's Web servers certified by trusted authorities that issue digital certificates.

The Heartbleed vulnerability effects specific versions of OpenSSL 1.0. It exploits the working memory of the Heartbeat Extension of OpenSSL to reveal up to 64 kilobytes of data in every periodic signal sent by the application. This can enable attackers to obtain private keys used to secure Internet traffic and decrypt Web, email, messaging and VPN communications. It can also be exploited to mount man-in-the-middle and session hijacking attacks. The vulnerability can be removed by upgrading to release 1.0.1g which includes bounds checks in the Heartbeat extension. The alternative is to recompile OpenSSL with the command -DOPENSSL_NO_HEARTBEATS to remove support for the Heartbeat extension. However, this may impact keep-alive connections.

Note 20055441 includes a link to SAP Knowledge Base Article (KBA) 2004805 that provides detailed information on application areas impacted by the Heartbleed vulnerability including Business Warehouse, Business Intelligence, Afaria and Mobile servers, and certain industry solutions. Note 2006177 includes procedures for checking OpenSSL versions in SUSE Linux Enterprise Servers that support SAP Business One. Note 2007688 provides details of multiple Sybase products vulnerable to Heartbleed.



SAP Security Notes by Vulnerability Type

Notes 1975842 and 2001778 introduce enhancements to improve the security of SAP BusinessObjects Mobile by removing support for self-signed certificates and generating alerts for sensitive operations in iOS and Android devices.

Note 1778940 patches a high priority verb tampering vulnerability in the Java application License Auditing Services. Similar to other Java Enterprise Edition (Java EE) platforms, the SAP J2EE supports verb-based or HTTP method authentication and access control through web.xml configuration files. Security constraints within such files can be used to restrict access requests to specific roles or users and deny requests from all other groups. Such mechanisms are often vulnerable to access bypass if applications support arbitrary or non-standard HTTP methods. A partial solution is to block requests that use non-standard methods.

Finally, although Note 1986895 carries a relatively low priority level, it deals with a vulnerability in the SAProuter network interface responsible for filtering SAP connections that could be exploited to obtain sensitive landscape information including host names, configuration data and user passwords. Therefore, the implementation of the relevant support package is highly recommended.

Appendix: SAP Security Notes, April 2014 1/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2007688	BC-SYB-OS	OpenSSL vulnerability (Heartbleed bug) in multiple SAP Sybase products
HOT NEWS	2006177	SBO-BC	Upgrade to a non-vulnerable OpenSSL version to resolve Heartbleed Bug in Business One installations
HOT NEWS	2005441	XX-SER-BO-SEC	Heartbleed (CVE-2014-0160) OpenSSL Vulnerability Â– Notification
HIGH	1971516	SV-SMG-SDD	Code injection vulnerability in SV-SMG-SDD
HIGH	1974016	BW-SYS-DB-DB4	Missing authorization check in function modules of BW-SYS-DB-DB4
HIGH	1974046	BC-ESI-ESF-BSA	Potential information disclosure relating to Business Data
HIGH	1600105	FIN-FSCM-BNK-SWF	Directory traversal in SWIFT file adapter
HIGH	1975842	MOB-APP-BI-IOS	Security Improvements for MOB-APP-BI-IOS
HIGH	1983739	CRM-BTX-BF-FIN	Hard-coded credentials in CRM-BTX-BF-FIN
HIGH	1985100	BC-DWB-TOO-CLA	Code injection vulnerability in Class Enhancements
HIGH	1878371	BC-SEC-SAL	Security Note for Security Audit Log
HIGH	1940405	SV-SMG-UMP	Code injection vulnerability in SV-SMG-UMP
HIGH	1929473	EP-PCT-MGR-CO	Hard-coded credentials in EP-PCT-MGR-CO
HIGH	1778940	XX-SER-LAS	HTTP verb tampering issue in SAP_JTECHS
HIGH	2001778	MOB-APP-BI-AND	Security Improvements for MOB-APP-BI-AND
HIGH	1073396	IS-B-BCA-AM	Missing authorization check in account management
HIGH	1590834	FIN-SEM-BPS-PLA	Update #1 to Security Note 1495333
HIGH	1993349	HAN-AS-XS-ADM	Unauthorized modification of displayed content in SAP HANA XS Administration Tool
HIGH	1987413	SRM-EBP-ADM-USR	Missing authorization check in User get list

Appendix: SAP Security Notes, April 2014 2/2

PRIORITY	NOTE	AREA	DESCRIPTION
HOT NEWS	2000095	BC-WD-ABA	Update 1 to Security Note 1812543
MEDIUM	1997862	BC-MID-ICF	Update 1 to security note 1334907
MEDIUM	1826001	BI-RA-WBI	Potential remote code execution in Webi Rich Client
MEDIUM	1583685	CA-GTF-PCF	Potential disclosure of persisted data in CRM-PCF
LOW	1815228	BC-SEC-LGN	Certificate Mapping: constraint "min. date" without function
LOW	1986895	BC-CST-NI	Potential disclosure of information in SAProuter

LAYER SEVEN SECURITY

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