April 14, 2014

Oracle Security Analysis

Heartbleed (CVE-2014-0160) and Oracle E-Business Suite

Summary

Oracle E-Business Suite environments may or may not be vulnerable to the **"Heartbleed" OpenSSL vulnerability (CVE-2014-0160)** depending on the deployment architecture. Oracle has released guidance in Oracle Support Note ID 1645479.1 "OpenSSL Security Bug-Heartbleed" *(support login required)* unequivocally stating Oracle E-Business Suite is not vulnerable. However, many Oracle E-Business Suite environments are architected in such a way that SSL termination is not performed on the Oracle E-Business Suite application servers, rather SSL termination is performed by load balancers, reverse proxies, or SSL accelerators. The Oracle E-Business Suite environment architecture must be reviewed to determine where the SSL termination point is.

- If the SSL termination point is the Oracle E-Business Suite application server using the bundled application server components (Oracle Application Server or Oracle Fusion Middleware), then the Oracle E-Business Suite environment is not vulnerable as older non-vulnerable versions of OpenSSL are used or non-OpenSSL components are used depending the version of Oracle E-Business Suite.

- If the SSL termination point is a load balancer, reverse proxy, or SSL accelerator, then the environment **MAY BE VULNERABLE** to the Heartbleed OpenSSL vulnerability. There are multiple recommended and often deployed products, such as F5 Big-IP and Apache with OpenSSL, which are vulnerable.

This analysis will detail where OpenSSL is commonly used in Oracle E-Business Suite environments and where vulnerable versions of OpenSSL may be found. The scope of this analysis is (1) commonly deployed architectures of Oracle E-Business Suite and (2) core components of Oracle E-Business Suite. Common Oracle E-Business Suite add-on components such as Oracle Discoverer, Oracle Business Intelligence Enterprise Edition (OBIEE), Oracle Internet Directory/Identify Management, and Oracle Fusion Middleware for SOA are out of scope for the purpose of this analysis and should be individually reviewed to determine if they are vulnerable.

To summarize, SSL and encrypted communication is commonly used in an Oracle E-Business environment in a number of places:

(1) HTTPS communication from the client browser to the Oracle E-Business Suite application server running Oracle Application Server 9iAS (11.5.x), Oracle Application Server 10.1.3 (12.0 and 12.1), or Oracle Fusion Middleware 11.1 (12.2)	**Not vulnerable** *(see below)*	The deployed SSL components for Oracle Application Server 9iAS, Oracle Application 10.1.3, and Oracle Fusion Middleware 11.1utilize older, non-vulnerable versions of OpenSSL or do not use OpenSSL.
(2) HTTPS communication from the client browser to load balancer, reverse proxy, or SSL accelerator	**May be vulnerable** *(see below)*	Depending the products used for load balancers, reverse proxies, or SSL accelerators, the Oracle E-Business Suite environment may be vulnerable. These products, such as F5 Big-IP load balancers or Apache reverse proxies, must be reviewed to determine if they are vulnerable.
(3) HTTPS communication from a load balancer or reverse proxy to an Oracle E-Business Suite application server	**Not vulnerable**	A limited number of organizations require all traffic to be encrypted and use SSL encryption between the load balancer/reverse proxy and the Oracle E-Business Suite application servers. The server component is the Oracle E-Business Suite application server, thus is not vulnerable.
(4) SSL Encrypted SQL*Net communication from the application server to the database server	**Not vulnerable**	The Oracle Database does not utilize OpenSSL for SSL/TLS support in the Advanced Security Option (ASO/ANO).
(5) Encrypted Forms Server socket mode (non-default mode) communication between the client and the Forms Server	**Not vulnerable**	The Forms Server socket mode (non-default mode) traffic can be encrypted, but utilizes a custom 40-bit encryption rather than SSL. The Forms Server running in Servlet mode utilizes the standard Oracle E-Business Suite application server web port.

Oracle E-Business Suite 11i (11.5.7 – 11.5.10.2)

The SSL implementation on the Oracle E-Business Suite 11i application server utilizes mod_ssl, which is based on OpenSSL. The OpenSSL libraries are statically linked in mod_ssl and version 0.9.5a is used. The base install of Oracle E-Business Suite includes the OpenSSL 0.9.5a binary, which is not vulnerable. The application server may be updated and patched to 1.0.2.2.2 (November 2005), which includes the same versions of OpenSSL and mod_ssl. The last available Critical Patch Update for the application server is October 2012 and includes updated versions of both the OpenSSL binary and mod_ssl to fix specific security vulnerabilities, but does not update the overall version of OpenSSL.

For more information on SSL with Oracle E-Business Suite 11i, see Oracle Support Note ID 123718.1 "11i: A Guide to Understanding and Implementing SSL for Oracle Applications."

Oracle E-Business Suite R12 (12.0 and 12.1)

In Oracle E-Business Suite R12, Oracle transitioned from using OpenSSL and mod_ssl to using mod_ossl and the Oracle Wallet. Mod_ossl is a derivative of mod_ssl based on OpenSSL, Certicom, and RSA libraries. Portions of the OpenSSL libraries are statically linked in mod_ossl and version 0.9.6a is used. Other than mod_ossl, there is no other installation of OpenSSL within R12. The Oracle Application Server 10.1.3 installed with Oracle E-Business Suite R12 may be upgraded to 10.1.3.5 and the same OpenSSL version 0.9.6a is statically linked in mod_ossl. The last available Critical Patch Update for the application server is July 2013 and does not update mod_ossl.

For more information on SSL with Oracle E-Business Suite R12, see Oracle Support Note ID 376700.1 "Enabling SSL in Oracle E-Business Suite Release 12."

Oracle E-Business Suite R12 (12.2)

Oracle E-Business Suite 12.2 includes support for Oracle Fusion Middleware 11g and Oracle WebLogic Server 10.3.6. The Oracle HTTP Server is still used as the web server and has been updated to 11.1.1.6, which is equivalent to Apache 2.2.21. In the Oracle E-Business Suite 12.2 application server installation, there is no inclusion of OpenSSL and it appears all references to statically linked OpenSSL in mod_ossl have been removed.

For more information on SSL with Oracle E-Business Suite R12, see Oracle Support Note ID 1367293.1 "Enabling SSL in Oracle E-Business Suite Release 12.2."

Load Balancers, Reverse Proxies, and SSL Accelerators

Many Oracle E-Business Suite environments are architected in such a way that SSL termination is not performed on the Oracle E-Business Suite application servers, rather SSL termination is performed by a load balancer, reverse proxy, or SSL accelerator. Also, SSL termination may be performed on different devices internally and externally (DMZ). Oracle recommends a number of load balancing and reverse proxy solutions for the Oracle E-Business Suite through various Oracle Support Notes. For Oracle E-Business Suite, commonly used products are F5 Big-IP, Cisco ACE Application Control Engine, BlueCoat ProxySG, Oracle Webcache, and Apache and usually act as the SSL termination point. These products may use vulnerable OpenSSL versions.

Oracle does provide instructions for building an Apache-based reverse proxy server for Oracle E-Business Suite 11i and R12 in Oracle Support Note ID 1190043.1 "Building an Apache 2.2 based Reverse Proxy from Source." Step 4 of this document give instructions on implementing OpenSSL for SSL support. The exact commands in this document install OpenSSL version 1.0.0, but we have to assume an experienced system administrator or DBA would install the latest version of OpenSSL. If installed or updated after March 2012, this would be OpenSSL version 1.0.1 to 1.0.1f, which are vulnerable. An Apache-based reverse proxy could also be built by an experienced system administrator using standard package management (e.g., rpm, yum, apt-get), thus installing the latest versions of Apache and OpenSSL at the time. Apache-based reverse proxy servers used with Oracle E-Business Suite should be diligently reviewed to determine if they are affected by the Heartbleed vulnerability.

For load balancing and reverse proxy products, please refer to the vendor for information if the product is affected by the Heartbleed vulnerability. We have included relevant references for products Integrigy encounters most often during our security assessments.

Product	Status	Security Advisory/References
F5 Big-IP	**Vulnerable versions 11.5.0 -11.5.1**	http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15159.html
BlueCoat ProxySG	**Vulnerable versions 6.5.1.1 - 6.5.3.5**	http://kb.bluecoat.com/index?page=content&id=SA79&actp=RSS
Cisco ACE Application Control Engine	**Not vulnerable**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

References

Heartbleed Vulnerability

- Oracle Support Note “OpenSSL Security Bug-Heartbleed” (Doc ID 1645479.1)

Oracle E-Business Suite and SSL

- Oracle Support Note “11i: A Guide to Understanding and Implementing SSL for Oracle Applications” (Doc ID 123718.1)
- Oracle Support Note “Enabling SSL in Oracle E-Business Suite Release 12.2” (Doc ID 1367293.1)
- Oracle Support Note “Enabling SSL in Oracle E-Business Suite Release 12” (Doc ID 376700.1)

Oracle E-Business Suite Load Balancing and Reverse Proxies

- Oracle Support Note “DMZ Configuration with Oracle E-Business Suite 11i” (Doc ID 287176.1)
- Oracle Support Note “Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i” (Doc ID 217368.1)
- Oracle Support Note “Oracle E-Business Suite R12 Configuration in a DMZ” (Doc ID 380490.1)
- Oracle Support Note “Installing and Configuring Web Cache 10g and Oracle E-Business Suite 12” (Doc ID 380486.1)
- Oracle Support Note “Installing and Configuring Web Cache 10.1.2 and Oracle E-Business Suite 11i” (Doc ID 306653.1)
- Oracle Support Note “Case History: Implementing a Reverse Proxy Alone in a DMZ Configuration - R12” (Doc ID 726953.1)
- Oracle Support Note “Case History: Implementing a Reverse Proxy Alone in a DMZ Configuration - 11i” (Doc ID 438744.1)
- Oracle Support Note “Building an Apache 2.2 based Reverse Proxy from Source” (Doc ID 1190043.1)

Note: An Oracle Support login is required for all Oracle Support Notes.

History

April 10, 2014 – Initial Internal Analysis
April 11, 2014 – Internal Draft
April 14, 2014 – Published

About Integrigy

Integrigy Corporation is a leader in application security for enterprise mission-critical applications. AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations. AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite. Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60602 USA
888/542-4802
www.integrigy.com

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Integrigy's Vulnerability Disclosure Policy – Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that is publicly available or readily discernible. We do not publish or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.