INTEGRIGY

October 15, 2014

Oracle Security Analysis

SSLv3 POODLE (CVE-2014-3566) Vulnerability and Oracle E-Business Suite

SUMMARY

Oracle E-Business Suite environments may be vulnerable to the recently disclosed **"POODLE" SSLv3 vulnerability (CVE-2014-3566)** depending on where SSL termination is performed for the application. Integrigy believes this to be a low to medium risk issue for Oracle E-Business Suite customers, especially those with Internet facing DMZ nodes. The primary impact would be a "man in the middle" attack between an Oracle E-Business Suite user (such as in a coffee shop) and the application. This would allow the attacker to view all traffic between the user and the application, including the user's Oracle EBS password.

Integrigy has confirmed all currently supported versions of the Oracle E-Business Suite (EBS) are vulnerable if the standard Oracle EBS SSL configuration is used and the SSL termination is performed natively by the Oracle E-Business Suite.

Oracle E-Business Suite may also be vulnerable to the POODLE vulnerability if a load balancer (such as F5 BIG-IP) or a reverse proxy is used as the SSL termination point and SSLv3 is configured. Our testing of Oracle E-Business Suite environments showed 95% have SSLv3 configured, thus vulnerable.

The following versions of the E-Business Suite are all vulnerable to POODLE:

- Oracle E-Business suite 11.5.10
- Oracle E-Business suite 12.0 and 12.1
- Oracle E-Business suite 12.2

Solution

The solution is to disable the use of the SSLv3 protocol (and also SSLv2 due to previously disclosed vulnerabilities) and use only TLS 1.0, 1.1, and 1.2. The only impact of disabling SSLv3 is compatibility with Internet Explorer 6. IE6 was desupported for Windows XP in April 2014, however, it is still supported on Windows Server 2003 until July 2015. IE6 users will not be able to connect to a website that is not running SSLv2 or SSLv3.

Native Oracle E-Business Suite SSL for Oracle E-Business Suite 11i

Oracle E-Business Suite 11.5.10 uses mod_ssl 2.8.1 and supports TLS 1.0. The SSLProtocol directive is not explicitly set in the Oracle EBS configuration files, therefore, the default is "SSLProtocol all". This will configure SSLv2, SSLv3, and TLS 1.0.

The SSL Protocol directive must be explicitly defined and only include TLS 1.0. This can only be accomplished by adding the following lines to the ***custom_apache.conf*** file in the Apache configuration directory as follows –

```
<IfDefine SSL>
<VirtualHost _default_:443>
      SSLProtocol    -all +TLSv1
</VirtualHost>
</IfDefine>
```

The **443** must be replaced with the SSL port number you are using. This is a work-around as this value is set via an AutoConfig parameter in ***httpd.conf***, but ***custom_apache.conf*** is not an AutoConfig controlled file.

Native Oracle E-Business Suite SSL for Oracle E-Business Suite 12.0 and 12.1

In Oracle E-Business Suite 12.0 and 12.1, the SSL protocols are set as follows in the ***ssl.conf*** file and cannot be set using an AutoConfig variable –

```
SSLProtocol    -all +TLSv1 +SSLv3
```

The "+SSLv3" option must be removed. This can only be accomplished by adding the following lines to the ***custom.conf*** file in the Apache configuration directory as follows –

```
<IfDefine SSL>
```

```
<VirtualHost _default_:443>
      SSLProtocol    -all +TLSv1
</VirtualHost>
</IfDefine>
```

The **443** must be replaced with the SSL port number you are using. This is a work-around as this value is set via an AutoConfig parameter in ***ssl.conf***, but ***custom.conf*** is not an AutoConfig controlled file.

Native Oracle E-Business Suite SSL for Oracle E-Business Suite 12.2

As Oracle E-Business Suite 12.2 is utilizing WebLogic Server for the application tier, therefore, the SSL configuration is different than previous versions of Oracle EBS.

Follow the instructions in Section 5 of My Oracle Support Note ID 1367293.1 "Enabling SSL in Oracle E-Business Suite Release 12.2." In the Fusion Middleware documentation Section 6.4.3.1 Step 5, you can specify the SSL protocols under "SSL Protocol Version". The value should be "nzos_Version_1_0" which will set TLS 1.0 and no other protocols. For Fusion Middleware, SSLv3 is "nzos_Version_3_0".

Load Balancer or Reverse Proxy

Review the documentation for the load balancer or reverse proxy for instructions on disabling SSLv3. If using an F5 BIG-IP load balancer, please see "CVE-2014-3566: Removing SSLv3 from BIG-IP" (https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip) for more information.

References

POODLE Vulnerability

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
- "This POODLE Bites: Exploiting The SSL 3.0 Fallback," https://www.openssl.org/~bodo/ssl-poodle.pdf
- "CVE-2014-3566: Removing SSLv3 from BIG-IP," https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip

History

October 10, 2014 – Initial Internal Analysis
October 13, 2014 – Internal Draft
October 15, 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.

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 are 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.