Oracle Security Alert #62
Dated: 4 December 2003
Severity: 1

SSL Update for CERT CA-2003-26 and older SSL issues

Description

This alert addresses SSL vulnerabilities detailed in CERT Advisory CA-2003-26, and SSL vulnerabilities detailed in several older Common Vulnerabilities and Exposures (CVE) candidates , as follows:

- CERT CA-2003-26 documents SSL vulnerabilities that can be exploited when carefully crafted X.509 certificates are presented by clients, even when X.509 client certificates are not enabled. The CVE numbers for these issues are CAN-2003-0544 and CAN-2003-0545.

- CERT CA-2003-26 also documents a vulnerability that is only present when processing of X.509 client certificates is enabled. The CVE number for this issue is CAN-2003-0543. This vulnerability affects all products that use SSL and accept client certificates in the Oracle9*i* Application Server, the Oracle9*i* Database Server, and the Oracle8*i* Database Server.

- The patches provided in this alert also fix the following older CVE issues: CVE-2002-0082, CAN-2003-0078, CAN-2003-0147, and CAN-2003-0131.

Products Affected

- Oracle9*i* Database Server Release 2, Version 9.2.0
- Oracle9*i* Database Server Release 1, Version 9.0.1
- Oracle8*i* Database Server Release 3, Version 8.1.7
- Oracle9*i* Application Server Version 9.0.2
- Oracle9*i* Application Server Version 9.0.3
- Oracle9*i* Application Server Release 1, Version 1.0.2.2
- Oracle9*i* Application Server Release 1, Version 1.0.2.1s
- Oracle HTTP Server Version 9.2
- Oracle HTTP Server Version 9.0.1
- Oracle HTTP Server Version 8.1.7

Platforms Affected

See Patch Availability Matrix (below).

Required conditions for exploit

Use of SSL with vulnerable products. Some of these vulnerabilities are not dependent on enabling Client certificates.

Risk to exposure

Risk to exposure is high. Any client that is able to access the server may exploit the vulnerabilities. The CERT advisory explains this in more detail.

How to minimize risk

Minimize risk by applying the patch(es). There are no workarounds that fully address these potential security vulnerabilities. Follow best practices for Oracle9*i* Application Server and Oracle9*i* Database Server, and consider deployment of firewalls.

http://otn.oracle.com/products/ias/pdf/best_practices/security_best_practices.pdf
http://otn.oracle.com/deploy/security/oracle9ias/pdf/securingias.pdf
http://otn.oracle.com/deploy/security/oracle9i/pdf/9ir2_checklist.pdf
http://otn.oracle.com/deploy/security/oracle9i/pdf/9i_checklist.pdf

Ramification for Customer

Oracle strongly recommends applying the patch for these vulnerabilities. Oracle recommends that customers review the severity rating for this Alert and patch accordingly. See

http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf

for a definition of severity ratings.

Workaround

There are no workarounds for these issues.

Patch Information

If there are two patches listed for the chosen product and platform in the **Patch Availability Matrix**, both must be downloaded and applied. The patches provided address all issues specified in this alert. Patches are available for the following products:

- Oracle9*i* Database Server Release 2, Version 9.2.0.4
- Oracle9*i* Database Server Release 2, Version 9.2.0.3
- Oracle9*i* Database Server Release 1, Version 9.0.1.4
- Oracle8*i* Database Server Release 3, Version 8.1.7.4
- Oracle9*i* Application Server Release 1, Version 1.0.2.2
- Oracle9*i* Application Server Release 1, Version 1.0.2.1s

Customers that use Oracle HTTP Server Version 9.2, 9.0.1, or 8.1.7 should apply patch number **3169446**.

Patches for Oracle9*i* Application Server Version 9.0.2 and 9.0.3 will be available in December, 2003.

Oracle E-Business Suite Release 11i customers can apply the patches listed in the **Patch Availability Matrix** to existing environments.

Patch Availability

Please see Metalink Document ID 249034.1:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=249034.1

for the patch download procedures and for the **Patch Availability Matrix** for this Oracle Security Alert.

Please review Metalink, or check with Oracle Support Services periodically for patch availability if the patch for your platform is unavailable. Oracle strongly recommends that you backup and comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0082
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0078
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0131
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0147
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0543
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0544
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0545
http://www.openssl.org/news/secadv_20030930.txt
http://www.uniras.gov.uk/vuls/2003/006489/openssl.htm
http://www.cert.org/advisories/CA-2003-26.html

Credits

Oracle acknowledges NISCC (www.niscc.gov.uk) for bringing these security vulnerabilities to Oracle's attention.

Modification History

04-DEC-03: Initial release, Version 1