

US-CERT Technical Cyber Security Alert TA04-160A -- SQL Injection Vulnerabilities in Oracle E-Business Suite

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2004-06/0001.html>

From: CERT Advisory (cert-advisory_at_cert.org)

Date: 06/08/04

Date: Tue, 8 Jun 2004 14:38:42 -0400

To: cert-advisory@cert.org

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Technical Cyber Security Alert TA04-160A
SQL Injection Vulnerabilities in Oracle E-Business Suite

Original release date: June 8, 2004

Last revised: --

Source: US-CERT

Systems Affected

- * Oracle Applications 11.0 (all releases)
- * Oracle E-Business Suite 11i, 11.5.1 through 11.5.8

Overview

A vulnerability in the Oracle's E-Business Suite allows a remote attacker to execute arbitrary script on a vulnerable database system. Exploitation may lead to compromise of the database application, data integrity, or underlying operating system.

I. Description

Oracle E-Business Suite is a set of applications and modules that enables an organization to manage customer interactions, deliver services, manufacture products, ship orders, collect payments, and other tasks using a single database model.

According to the Oracle Security Alert 67, Oracle Applications 11.0 (all releases) and Oracle E-Business Suite Release 11i, 11.5.1 through 11.5.8 are vulnerable to SQL injection vulnerabilities. Oracle E-Business Suite Release 11.5.9 and later are not vulnerable. This

vulnerability is not platform specific. Integriqy Corporation has also released an alert about these vulnerabilities.

Note that no authentication mechanisms of Oracle E-Business Suite will mitigate exploitation of the attack.

US-CERT is tracking this issue as VU#961579.

II. Impact

An unauthenticated attacker could exploit this vulnerability to execute arbitrary SQL statements on the vulnerable system with the privileges of the Oracle server process. In addition to compromising the integrity of the database information, this may lead to the compromise of the database application and the underlying operating system.

III. Solution

Apply Patch or Upgrade

According to the Oracle Security Alert 67, patches and related information are available from:

http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocuments?p_database_id=NOT&p_id=274375.1

Appendix B. References

- * <http://otn.oracle.com/deploy/security/pdf/2004alert67.pdf>
- * <http://www.integriqy.com/alerts/OraAppsSQLInjection.htm>
- * <http://www.kb.cert.org/vuls/id/961579>

US-CERT thanks Stephen Kost of Integriqy Corporation for reporting this problem and for information used to construct this advisory.

Feedback can be directed to the author: Jason A. Rafail

The latest version of this document can be found at:

<<http://www.us-cert.gov/cas/techalerts/TA04-160A.html>>

Copyright 2004 Carnegie Mellon University.

Terms of use:

<<http://www.us-cert.gov/legal.html>>

Revision History

June 8, 2004: Initial release

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.1 (GNU/Linux)

iD8DBQFAxgVFXIvNRxAkFWARAiZSAKCsoyCrmSth7nWRX62FPnYZRUXp3QCeI5f+
gOYuIony8dN59HQ+63PUIMw=
=k4uL

-----END PGP SIGNATURE-----