Oracle Security Alert #37
Created: 1 August, 2002
Updated: 5 August, 2002
Updated: 9 August, 2002
Updated: 24 September, 2002

OpenSSL Security Vulnerability

Description:

There are remotely exploitable buffer overflow vulnerabilities in OpenSSL versions prior to 0.9.6e.
These vulnerabilities may allow a remote attacker to execute arbitrary code or perform a denial-of-service (DoS) attack.

These problems are described in the OpenSSL Security Advisory [30 July 2002].
These problems are also described in CERT® Advisory CA-2002-23.
The steps listed in this Security Alert also protect against the Apache/mod_ssl worm, descrbed in CERT® Advisory CA-2002-27.

Products affected:

- Oracle HTTP Server (OHS) shipped with the database up to and including version 9.2.0.
- Oracle9*i*AS versions earlier than 9.0.2, including all versions 1.0.2.x.

CorporateTime Outlook Connector (CTOC), versions 3.1, 3.1.1, 3.1.2, and 3.3 on Windows 98, NT, 2K, XP.

Workarounds:

There are no workarounds against the potential denial-of-service attack. Disabling SSL should prevent remote execution of code.

Users of Corporate Time Outlook Connector can disable TLS by adding the following section to the CTOC.INI file:

```
[CTOC]
allow-tls=FALSE
```

NOTE:

Disabling SSL or TLS will result in data being transmitted in the clear (i.e. unencrypted), *including passwords* whenb using Basic Authentication.

Patch Information:

Download currently available patches for your platform from the Oracle Support Services web site, MetaLink:

1. Activate the "Patches" button to get the the patches web page.
2. Enter patch 2492925 and activate the "Submit" button.

Upgrade Information:

New releases of the Corporate Time Outlook Connector will address this vulnerability.

- CorporateTime Outlook Connector 3.3.1
- Oracle Outlook Connector 3.4
