Oracle Security Alert #43
Dated: 04 October 2002
Severity: 3

Oracle9*i* Application Server - Web Cache Administration Tool Crash on Malformed Request

Description
A potential security vulnerability has been discovered in the Oracle9*i*AS Web Cache administration module also known as the Web Cache Manager tool, on the Windows platform. If a malicious and knowledgeable user sends either of the following requests to the port on which the Web Cache administration process is listening, the administration process will crash resulting in a Denial of Service (DoS) against the administration module.

Request 1:

```
GET /../ HTTP/1.1
host: hostname
Enter
Enter
```

Request 2:

```
GET /some.html/ HTTP/1.1
host: host name
Transfer Encoding
Enter
Enter
```

This behavior reproduces consistently on Windows. This behavior does not manifest on Unix platforms. Note that the administration process is the only process affected. The cache process is not affected.

Products affected
Web Cache technology in Oracle9*i* Application Server, Release 9.0.2.

Platforms affected
Windows only (Unix platforms not affected)

Patch Information
No patch is available at present for this potential security vulnerability. Customers should follow best security practices for protecting the administration process from unauthorized users and requests. As such, Oracle strongly encourages customers to take both of the following protective measures:

1. Use firewall techniques to restrict access to the Web Cache administration port.
2. Use the “Secure Subnets” feature of the Web Cache Manager tool to provide access only to administrators connecting from a list of permitted IP addresses or subnets.

The potential security vulnerability is being tracked internally at Oracle and will be fixed by default in the 9.0.4 release of Oracle9*i* Application Server.

Credits
Oracle Corporation thanks Andreas Junestam of @Stake for discovering this potential security vulnerability and promptly bringing it to Oracle’s attention.