**Oracle Security Alert #52**
**Dated: 11 February 2003**
**Updated: 03 March 2003**
**Severity: 2**

**Two Vulnerabilities in Oracle9*i* Application Server**

**Description**

**1. DAV_PUBLIC Directory**
A potential security vulnerability has been discovered in Oracle9*i* Application Server. A knowledgeable and malicious user can cause a Denial of Service (DoS) attack by exploiting an exposed directory in Orace9*i* Application Server.

**Products Affected**
Oracle9*i* Application Server Release 9.0.2.

**Platforms Affected**
All the Oracle9*i* Application Server supported platforms (Solaris, Linux, HP-UX, AIX, HP Tru64, Windows NT/2000).

**Required conditions for exploit**
An installation of Oracle9iAS. Authentication is **not** required.

**Risk to exposure**
Not as high as the database server vulnerabilities even though exploit is possible via Internet or Intranet. Crafting an exploit to take advantage of exposed URL requires specialized knowledge.

**How to minimize risk**
Relatively simply workaround addresses the issue. Also, follow best practices for 9iAS, http://otn.oracle.com/deploy/security/oracle9iAS/pdf/securingias.pdf (note that this document is for Oracle9iAS Release 1.0.2.x but concepts can be applied to 9iAS Release 9.0.2 as well. Best practice for 9iAS Release 9.0.2 is in progress.)

**Ramification for CUSTOMER**
Apply workaround to all Oracle9iAS installations after applying patch for issue #2 in this Alert. See http://otn.oracle.com/deploy/security/pdf/oracle_severity_ratings.pdf for a definition of severity ratings.

**Workaround**
Oracle strongly urges customers to apply the following workaround to address this vulnerability.

Edit the **moddav.conf** file located in ORACLE_HOME/Apache/oradav/conf as follows:

Change the line:

DAV on

To:

DAV off

After closing the file, the resulting configuration file should now read:

```
Load/Module ORACLE_HOME/Apache/oradav/lib/mod_oradav.so

#This is needed by mod_oradav to manage locks on WebDAV activity
#against a local file system and contains lock information about all
#WebDAV file resources.

DAVLockDB ORACLE_HOME/Apache/oradav/var/DAVLock

<Location/dav_public>
DAV off

#For extra security, enable the ForceType directive below.
#ForceType is used to prevent any scripts (jsp,php,...)
#from being run.  Since this is a public location and anyone
#could upload a script and then execute it we need to be
#careful - we don't want it exploited.  To preserve
#mime types of files but to still protect against executables
#see HTTP Admin Documentation on mod_oradav regarding
ORAGetSource.
#
#ForceType text/plain

</Location>
```

**Patch Information**
Oracle has fixed the potential security vulnerability identified above in Oracle9*i* Application Server release 9.0.3. You must upgrade to release 9.0.3 if you do not want to implement the workaround in any of the pre-9.0.3 releases.

**Credits**
Oracle Corporation thanks David Litchfield of Next Generation Security Software Ltd. for discovering and promptly reporting this potential security vulnerability to Oracle's attention.

## 2. MOD_ORADAV Module

A potential security vulnerability has been discovered in Oracle9*i* Application Server. A knowledgeable and malicious user can exploit exposed URLs of Oracle9*i* Application Server and compromise the MOD_ORADAV module that may result in a remote Denial of Service (DoS) attack against Oracle9*i* Application Server.

**Product Affected**
Oracle9*i* Application Server Release 9.0.2 and Release 9.0.3.

**Platforms Affected**
All the Oracle9*i* Application Server supported platforms (Solaris, Linux, HP-UX, AIX, HP Tru64, Windows NT/2000).

**Required conditions for exploit**
An installation of Oracle9iAS. Authentication is **not** required.

**Risk to exposure**
Not as high as the database server vulnerabilities even though exploit is possible via Internet or Intranet. Crafting an exploit to take advantage of exposed URL requires specialized knowledge.

**How to mitigate**
Follow best practices for 9iAS,
http://otn.oracle.com/deploy/security/oracle9iAS/pdf/securingias.pdf
(note that this document is for Oracle9iAS Release 1.0.2.x but concepts can be applied to 9iAS Release 9.0.2 as well. Best practice for 9iAS Release 9.0.2 is in progress.)

**Ramification for CUSTOMER**
Patch affected application servers after patching Alert #51 but with higher priority than the workaround for issue #1 in Alert #52.

**Patch Information**
The fix for this potential security vulnerability is available for the Oracle9i Application Server at the latest patchset level (as listed in the **Fixed by** section) for each supported release on the platforms listed in the Patch Availability Matrix. **If you are not on the latest patchset release, you need to apply the latest patchset before applying this one-off patch.** Please note this fix will be included in the Oracle9i Application Server Release 9.0.4. by default.

**Fixed by**
An interim (one-off patch) for this issue is available for these affected iAS versions:

- Oracle 9*i* Application Server, version 9.0.2 on Solaris
- Oracle 9*i* Application Server, version 9.0.2 on Windows
- Oracle 9*i* Application Server, version 9.0.3 on Solaris
- Oracle 9*i* Application Server, version 9.0.3 on Windows

Download this one-off patch from the Oracle Support Services web site, MetaLink (http://metalink.oracle.com).

1. Click on the Patches button.
2. Click on the "New Metalink Patch Search ".
   If you are not on the "Simple Search" screen, click on the "Simple Search" button.
3. Input the bug number **2602262** on the "Search by Patch Number" box.
4. Click **Go**.
5. Select the patch for the appropriate product version.

6. Select the appropriate platform.
7. Click **Download**.

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 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.

**Patch Availability Matrix**

| Platforms | 9.0.2 | 9.0.3 |
|---|---|---|
| Sun Solaris (32-bit) | Available | Available |
| Sun Solaris (64-bit) | N/A | N/A |
| IBM AIX 4.3.3 (32-bit) | Planned | Planned |
| IBM AIX 4.3.3 (64-bit) | N/A | N/A |
| IBM AIX Based 5L (64-bit) | N/A | N/A |
| MS Windows NT/2000/XP | Available | Available |
| HP-UX (64-bit) | Planned | Planned |
| HP Tru64 | Planned | Planned |
| LINUX (RH 6.2) | Planned | Planned |
| LINUX (SUSE 7.1) | Planned | Planned |
| INTEL SOLARIS | N/A | N/A |
| DATA GENERAL | N/A | N/A |
| UNIXWARE | N/A | N/A |
| IBM NUMA-Q | N/A | N/A |
| SGI-IRIX-64 | N/A | N/A |
| Siemens-64 | N/A | N/A |
| Novell | N/A | N/A |
| OpenVMS | N/A | N/A |
| IBM OS/390 (MVS) | N/A | N/A |
| NEC | N/A | N/A |

**N/A:** A patch will not be created for that platform and version of Oracle Application Server.

**Planned:** The patchset is not released as yet. Future releases (e.g., 9.0.3 and higher) of the Oracle9*i* Application Server will contain the fix by default.

**Credits**

Oracle Corporation thanks David Litchfield and Mark Litchfield of Next Generation Security Software Ltd. for discovering and bringing this potential security vulnerability to Oracle's attention.

**Modification History**

21-Feb-2003: The Products Affected and Patch Information sections clarified.
26-Feb-2003: Required conditions, risk to exposure, how to minimize risk, and ramification for customer sections added.
03-Mar-2003: Title updates and minor updates to flow of text.