Oracle Security Alert #60
Dated: 28 October 2003
Severity: 2

Unauthorized Access to Restricted Content in Oracle Files

Description

A potential security vulnerability has been discovered in the Oracle Files component that ships with Oracle Collaboration Suite Release 1. A knowledgeable and malicious user of Oracle Files can potentially access restricted content.

In the Oracle Files component that ships with Oracle Collaboration Suite Release 1, Oracle WebCache has default cacheability rules for the following types of files: js, html, pdf, bmp/png, and jpg/jpeg. Releases previous to Oracle Files Release 9.0.3.3.6 did not override these cacheability rules. Interactions with the Oracle Files component and these rules can lead to the unauthorized access of restricted content by any user of Oracle Files.

Products Affected

- Oracle Files Release 9.0.3.1.x
- Oracle Files Release 9.0.3.2.0
- Oracle Files Release 9.0.3.3.x

NOTE: Oracle Files Release 9.0.4.1.x and later releases are **not** affected. E-business Suite is **not** affected.

Platforms Affected

All supported platforms.

Required conditions for exploit

Oracle Files authenticated user (i.e. valid login is required). Note that Oracle Files and WebCache are installed and enabled by default with Oracle Collaboration Suite.

Risk to exposure

Risk to exposure is medium because a potential exploit requires an authenticated user of Oracle Files, and the vulnerability can be eliminated by modifying caching rules. In the affected releases, Oracle WebCache has default cacheability rules that are excessively permissive. Releases previous to Oracle Files Release 9.0.3.3.6 do not override these cacheability rules and may thereby lead to the unauthorized access of restricted content by any authenticated user of Oracle Files.

How to minimize risk

Minimize risk by applying the Oracle Files Release 9.0.3.3.6 patch. Follow Oracle's best practices by consulting

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

and consider deployment of firewalls, etc.

Ramification for customers

Contents from a restricted folder may be compromised. Oracle strongly recommends applying the patch for this potential vulnerability. 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

Disabling Oracle WebCache will eliminate this potential vulnerability, because WebCache's default caching rules will no longer apply and the Files access controls then work unaffected by WebCache. For details on disabling WebCache, see the *Oracle9iAS WebCache Administration and Deployment Guide* [Chapter 8: Administering Oracle9*i*AS WebCache].

Patch Information

A patch (Oracle Files Release 9.0.3.3.6) for this issue is available for these affected Oracle Files versions:

- Oracle Files Release 9.0.3.1.x
- Oracle Files Release 9.0.3.2.0
- Oracle Files Release 9.0.3.3.x

The patch is platform independent and may be applied across all platforms on which Oracle Collaboration Suite is supported.

Fixed By

Download this patch from the Oracle Support Services web site, MetaLink <http://metalink.oracle.com>.

1. Click on the **Patches** button.
2. Click on "Simple Search".
3. In the "Search By" option select "Patch Numbers(s)" from the drop-down menu, and enter **3036419** in the box.
4. This is a generic patch, so there is no need to specify the platform.

5. Click on the “Go” button.
6. Click on the “Download” button.
7. Recommended: you should also click on the “View README” button for additional information and instructions.

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.

Special Note: This is a cumulative patch which contains several other important bug fixes (not security related) from previous patches, including data corruption bug fixes. Applying this patch alone is sufficient to get to the latest Oracle Files patch set. For the list of bugs click on “View README” button on the MetaLink page.

Modification History

28-OCT-03: Initial release, Version 1