UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−034

Actualización de Oracle para múltiples vulnerabilidades

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que Oracle ha liberado un parche para diversas vulnerabilidades en varios de sus productos. El impacto de estas vulnerabilidades incluyen ejecución de código arbitrario, fuga de información y negación de servicio.

Fecha de Liberación:	18 de Octubre de 2006
Ultima Revisión:	18 de Octubre de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Sistemas Afectados

JD Edwards EnterpriseOne Tools, OneWorld Tools	==8.95, 8.96
JD Edwards EnterpriseOne, OneWorld Tools	==SP23
Oracle Application Server 10g	==Release 1 version 10.1.2.0
Oracle Application Server 10g Release 2	==versions 10.1.2.0.0 − 10.1.2.0.2, 10.1.2.1.0
Oracle Containers for J2EE	==client−only installations
Oracle Database 10g	==Release 2, versions 10.2.0.1, 10.2.0.2
Oracle Database 10g Release 1	==versions 10.1.0.4, 10.1.0.5
Oracle E−Business Suite Release 11.0	==

Oracle E−Business Suite Release 11i	==
Oracle PeopleSoft Enterprise Tools	==8.22, 8.46, 8.47, 8.48
Oracle PeopleSoft Enterprise Tools	==Enterprise Portal, versions 8.8, 8.9
Oracle Pharmaceutical Applications	==4.5.0 − 4.5.1
Oracle Reports Developer	==client−only installations
Oracle8i Database Release 3	==version 8.1.7.4
Oracle9i Collaboration Suite Release 2	==version 9.0.4.2
Oracle9i Database	==Release 2, versions 9.2.0.6, 9.2.0.7

Riesgo

Alto

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

Oracle ha liberado su actualización de parches críticos de Octubre de 2006.

De acuerdo con Oracle, esta actualización de parches incluye:

- 22 actualizaciones de seguridad para Oracle Database
- 6 actualizaciones de seguridad para Oracle HTTP Server
- 35 actualizaciones de seguridad para Oracle Application Express
- 14 actualizaciones de seguridad para Oracle Application Server
- 13 actualizaciones de seguridad para Oracle E−Business Suite
- 8 actualizaciones de seguridad para Oracle PeopleSoft Enterprise PeopleTools y Enterprise Portal Solutions
- 1 actualización de seguridad para JD Edwards EnterpriseOne
- 1 actualización de seguridad para Oracle Pharmaceutical Applications

Diversos productos de Oracle incluyen o comparten código con otros componentes de Oracle vulnerables. En consecuencia, una vulnerabilidad puede afectar a múltiples productos y componentes de Oracle. Por ejemplo, la actualización de Octubre de 2006 no incluye ningún parche específico para Oracle Collaboration Suite. Sin embargo, Oracle Collaboration Suite es afectado por vulnerabilidades presentes en Oracle Database y Orale Application Server, así que los sitios que ejecuten Oracle Collaboration deben

instalar las actualizaciones para Oracle Database y Oracle Application Server. Favor de consultar los detalles del CPU (Critical Patch Update) de Octubre de 2006 para conocer las vulnerabilidades que afectan a componentes y productos específicos de Oracle.

Para obtener una lista de vulnerabilidades conocidas que son mitigadas en el CPU de Octubre de 2006, consultar el mapa de vulnerabilidades públicas de alertas/boletines.

El CPU de Octubre de 2006 no asocia identificadores de vulnerabilidades (ej. DB01) con otra información disponible, incluso en el mapa de vulnerabilidades públicas de alertas/boletines. Mientras tanto, conforme más detalles de las vulnerabilidades y estrategias de remediación se tengan disponibles, se actualizarán las notas individuales de cada vulnerabilidad.

II. Impacto

El impacto de estas vulnerabilidades varía dependiendo de cada producto, componente y configuración del sistema. Las consecuencias potenciales incluyen ejecución de código arbitrario y comandos, fuga de información sensible y negación de servicio.

Los componentes vulnerables pueden estar disponibles para usuarios remotos que no se han autenticado en el sistema. Un atacante que comprometa el servidor de bases de datos de Oracle podría obtener acceso a información sensible y tomar control total del sistema.

III. Solución

Aplicar los parches o actualizar tal como se especifica en la nota de parches y actualizaciones críticas del mes de Octubre del 2006. Cabe señalar que estas actualizaciones sólo muestran vulnerabilidades corregidas recientemente.

Como se muestra en la nota de la actualización, algunos parches son acomulativos, y otros no:

Los parches para la base de datos Oracle, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne, JD Edwards OneWorld Tools, PeopleSoft Enterprise Portal Applications y las herramientas empresariales PeopleTools de PeopleSoft son acumulativos; cada parche crítico contiene las correcciones de actualizaciones anteriores. Los parches para la suite y aplicaciones Oracle E−Business no son acomulativos, de manera que los clientes de la suite y aplicaciones E−Business deberán consultar las actualizaciones anteriores para identificar parches que deseen instalar.

La nota de parches críticos del mes de Octubre enumera 35 vulnerabilidades que afectan a la solución Oracle Application Express. Estas vulnerabilidades son corregidas en la versión 2.2.1 de Oracle Application Express. Se recomienda a los usuarios de Oracle Application Express actualizar a la versión 2.2.1 pronto.

Las vulnerabilidades descritas en la nota de Octubre del 2006 podrían afectar a la base de datos Oracle 10g Express Edition (XE). De acuerdo con Oracle, la base de datos XE está basada en el código de la base de datos Oracle 10g Release 2.

Los parches para algunas plataformas y componentes no estuvieron disponibles cuando la nota de seguridad se publicó el pasado 17 de Octubre del 2006. Por favor consulte el Metalink 391563.1 (requiere autenticación) para más información sobre la disponibilidad de los parches

Los problemas conocidos con los parches de Oracle están documentados en las notas de pre−instalación y en los archivos readme. Por favor consulte y verifique estos documentos antes de realizar cambios a los

sistemas de producción.

IV. Referencias

- Nota de vulnerabilidad del US−CERT acerca del Critical Patch Update − Octubre 2006 − http://www.kb.cert.org/vuls/byid?searchview_oct_2006
- Nota de actualizaciones críticas (Critical Patch Updates) − Octubre 2006 − http://www.oracle.com/technology/deploy/security/critical−patch−updates/cpuoct2006.html
- Actualizaciones críticas y alertas de seguridad http://www.oracle.com/technology/deploy/security/alerts.htm
- Tabla de boletines de alerta públicos http://www.oracle.com/technology/deploy/security/critical−patch−updates/public_vuln_to_advisory_m
- Checklist de seguridad para la base de datos Oracle (pdf) http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
- Mejores prácticas para la implantación de parches críticos (pdf) http://www.oracle.com/technology/deploy/security/pdf/cpu_whitepaper.pdf
- Descargas para Oracle Application Express 2.2 http://www.oracle.com/technology/products/database/application_express/download.html
- Metalink 391563.1 de Oracle http://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOTi>
- Oracle Database 10g Express Edition http://www.oracle.com/technology/products/database/xe/index.html
- Análisis de los parches críticos del mes de Octubre para RDBMS de Oracle http://www.databasesecurity.com/oracle/OracleOct2006−CPU−Analysis.pdf
- Detalles de actualizaciones críticas del mes de Octubre del 2006 http://www.red−database−security.com/advisory/oracle_cpu_oct_2006.html

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- David Jiménez Domínguez (djimenez at correo dot seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- Eduardo Espina (eespina at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E−Mail: seguridad@seguridad.unam.mx
http://www.cert.org.mx
http://www.seguridad.unam.mx
ftp://ftp.seguridad.unam.mx
Tel: 56 22 81 69
Fax: 56 22 80 43