UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletin de Seguridad UNAM-CERT-2007-025

Actualizaciones de Oracle para múltiples vulnerabilidades

Los productos y componentes de Oracle son afectados por múltiples vulnerabilidades. Los impactos de estas vuln
incluyen la ejecución remota de código, revelación de información y negación de servicio.

Fecha de Liberación:	17 de Octubre de 2007
Ultima Revisión:	18 de Octubre de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así c foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas afectados

- Oracle Database 10*g*
- Oracle 9*i* Database
- Oracle Enterprise Manager 10*g* Database Control
- Oracle Application Server 10*g*
- Oracle Collaboration Suite 10*g*
- Oracle PeopleSoft Enterprise
- Oracle E-Business Suite
- Oracle PeopleSoft Enterprise Human Capital Management

Para mayor informacin relacionada con los productos afectados, consulte Actualizacin de Parches Crticos - Oc
2007 de Oracle.

II. Descripción

Oracle ha liberado su Actualización de Parches Críticos Octubre de 2007. Esta actualización soluciona más d vulnerabilidades en diferentes productos y componentes.

La Actualización de Parches Críticos proporciona información sobre los componentes afectados, acceso y auto requerida y el impacto desde vulnerabilidades en confidencialidad, integridad y disponibilidad de datos. Los us MetaLink deberían referenciar a la Nota de MetaLink 394487.1 (inicio de sesión requerido) para mayor inform términos utilizados en la Actualización de Parches Críticos.

De acuerdo a Oracle, ninguna de las vulnerabilidades corregidas en la Actualización de Parches Críticos de Ora solamente las instalaciones del Cliente de Base de Datos de Oracle.

En la mayoría de los casos, Oracle no asocia identificadores Vuln# (por ejemplo, DB01) con otra información Si llegan a estar disponibles detalles adicionales sobre las vulnerabilidades y técnicas de solución, el US-CERT su Base de Datos de Notas de Vulnerabilidad .

III. Impacto

El impacto de estas vulnerabilidades varía dependiendo del producto, componente y configuración del sistema. Consecuencias potenciales incluyen la ejecución de código arbitrario o comandos, revelación de información y servicio. Los componentes vulnerables podrían estar disponibles para atacantes remotos no autenticados. Un at comprometa una base de datos de Oracle podría ser capaz de obtener acceso a información sensitiva.

IV. Solución

Aplicar un parche

Aplicar los parches o actualizaciones apropiadas como se especifica en la Actualización de Parches Críticos 2007 de Oracle. Debe notar que esta Actualización de Parches Críticos solo lista los problemas corregidos reci Las actualizaciones para parchar los problemas conocidos previamente no están listadas.

Como se hace notar en la actualización, algunos parches son acumulativos, otros no lo son:

> *Los parches para Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Cont Collaboration Suite, JD Edwards EnterpriseOne and OneWorld Tools, y PeopleSoft Enterprise Portal en las Actualizaciones son acumulativos; cada Actualización de Parche Critico contiene las solucione Actualizaciones de Parches Críticos anteriores.*
>
> *Los parches para Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Cont Collaboration Suite, JD Edwards EnterpriseOne and OneWorld Tools, y PeopleSoft Enterprise Portal en las Actualizaciones son acumulativos; cada Actualización de Parches Criticos contiene las solucion Actualizaciones de Parches Críticos anteriores.*
>
> *Los parches para Oracle E-Business Suite and Applications no son acumulativos, por lo que los usuar E-Business Suite and Applications deberían referirse a las Actualizaciones de Parches Críticos previa identificar las soluciones anteriores que necesitan aplican.*

Los parches para algunas plataformas y componentes no estuvieron disponibles cuando la Actualización de Par Críticos fue publicada el 17 de octubre de 2007. Consulte la Nota de MetaLink 360465.1 (inicio de sesión requ mayor información.

Los problemas conocidos con los parches de Oracle están documentados en las notas de preinstalación y los ar
readme de los parches. Consulte estos documentos específicos para su sistema antes de aplicar los parches.

V. Apéndice A. Información del distribuidor

Oracle

Consulte la Actualización de Parches Críticos Octubre de 2007 y Actualizaciones de Parches Críticos y Aleta
Seguridad.

VI. Apéndice B. Referencias

- Actualización de Parches Críticos Octubre de 2007 - <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuoct2007.html>
- Actualizaciones de Parches Críticos y Aletas de Seguridad - <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Mapeo de Vulnerabilidades Publicas a Avisos/Alertas - <http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html>
- Checklist de Seguridad de Base de Datos de Oracle (PDF) - <http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf>
- Nota de MetaLink 360465.1 (inicio de sesión) - <https://metalink.oracle.com/metalink/plsql/f?p=200:37:3865010496644547 00::::p_database_id,p_id,p
- Detalles de la Actualización de Parches Críticos de Oracle de Octubre de 2007 - <http://www.red-database-security.com/advisory/oracle_cpu_oct_2007.html>

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

- Jesús Ramón Jiménez Rojas (jrojas 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