UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−003

Actualización de Oracle para múltiples vulnerabilidades

Productos y componentes de Oracle son afectados por múltiples vulnerabilidades. El impacto de estas vulnerabilidades incluye la ejecución remota de código arbitrario, revelación de información y negación de servicio.

Fecha de Liberación:	17 de Enero de 2008
Ultima Revisión:	17 de Enero de 2008
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas Afectados

- Oracle Database 10g Release 2, versiones 10.2.0.2, 10.2.0.3
- Oracle Database 10g versión 10.1.0.5
- Oracle 9i Database Release 2, versiones 9.2.0.8, 9.2.0.8DV
- Oracle Application Server 10g Release 3 (10.1.3), versiones 10.1.3.0.0, 10.1.3.1.0, 10.1.3.3.0
- Oracle Application Server 10g Release 2 (10.1.2), versiones 10.1.2.0.2, 10.1.2.1.0, 10.1.2.2.0
- Oracle Application Server 10g (9.0.4), versión 9.0.4.3
- Oracle Collaboration Suite 10g versión 10.1.2
- Oracle PeopleSoft Enterprise versiones 8.22, 8.48, 8.49
- Oracle E−Business Suite versiones 12, versiones 12.0.0 − 12.0.3
- Oracle E−Business Suite versiones 11i, versiones 11.5.9 − 11.5.10 CU2

Para mayor información relacionada con los productos afectados, consulte **Actualización de Parches Críticos – Enero de 2008**.

II. Descripción

Oracle ha liberado su **Actualización de Parches Críticos – Enero de 2008**. Esta actualización soluciona 26 vulnerabilidades en diferentes productos y componentes Oracle.

La Actualización de Parches Críticos proporciona información sobre los componentes afectados, acceso y autorización requerida y el impacto de las vulnerabilidades en confidencialidad, integridad y disponibilidad de datos. Los usuarios de MetaLink deben acudir a la Nota de MetaLink **467880.1** (se requiere login) para mayor información sobre los términos utilizados en la Actualización de Parches Críticos.

De acuerdo a Oracle, ninguna de las vulnerabilidades corregidas en la Actualización de Parches Críticos de Oracle afecta las instalaciones Oracle Database Client−only.

En la mayoría de los casos, Oracle no asocia identificadores Vuln# (por ejemplo, DB01) con otra información disponible.

III. Impacto

El impacto de estas vulnerabilidades varía dependiendo del producto, componente y configuración del sistema. Las consecuencias potenciales incluyen la ejecución de código o comandos arbitrarios, revelación de información y negación de servicio. Los componentes vulnerables podrían estar disponibles para atacantes remotos no autenticados. Un atacante que 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 de Oracle de Enero de 2008.

Se debe notar que esta Actualización de Parches Críticos solo lista los problemas corregidos recientemente. Las actualizaciones para solucionar problemas anteriores no están listados.

Como se menciona en la actualización, algunos de estos parches son acumulativos y otros no lo son:

Los parches para Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle E−Business Suite Applications (Release 12 only), JD Edwards EnterpriseOne, JD Edwards OneWorld Tools, PeopleSoft Enterprise Portal Applications y PeopleSoft Enterprise PeopleTools en las Actualizaciones son acumulativos; cada una de las Actualizaciones de Parche Critico contiene las soluciones de las Actualizaciones de Parches Críticos Anteriores.

Los parches para Oracle E−Business Suite Applications Release 11i no son acumulativos, por lo que los usuarios de Oracle E−Business Suite Applications deberían referirse a las Actualizaciones de Parche Críticos previas para identificar las soluciones anteriores que necesitan aplicar. Los parches para Oracle Collaboration Suite son acumulativos, incluyendo los parches de Abiril de 2007 de La Actualización de Parches Criticos. Desde la Actualización de Parches Críticos de julio de 2007 en adelante, los parches de seguridad de Oracle Collaboration Suite se entregan usando la infraestructura de parches one−off usada normalmente por Oracle para ofrecer correcciones de errores únicas a los clientes.

Los parches para algunas plataformas y componentes no estuvieron disponibles cuando la Actualización de Prches Críticos fue publicada el 17 de Enero de 2008. Consulte la nota de MetaLink 467880.1 (se requiere login) para mayor información.

Los problemas conocidos con los parches de Oracle están documentados en las notas de instalación y los archivos 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 Oracle− Enero de 2008 y Actualizaciones de Parches Críticos y alertas de seguridad.

VI. Apéndice B. Referencias

1. Actualización de Parches Críticos Enero de 2008 http://www.oracle.com/technology/deploy/security/critical−patch−updates/cpujan2008.html
2. Actualización de parches Críticos y alertas de seguridad href="http://www.oracle.com/technology/deploy/security/alerts.htm
3. Mapa de Vulnerabilidad Pública para Avisos/Alertashttp://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapp
4. Checklist de Seguridad de Base de Datos de Oracle (PDF)href="http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
5. Nota de MetaLink 467880.1 (login)https://metalink.oracle.com/metalink/plsql/f?p=200:37:8541351131282773504::::p_database_id
6. Detalles de la Actualización de Parches Críticos de Oracle de Enero de 2008http://www.red−database−security.com/advisory/oracle_cpu_jan_2008.html

---

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

- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- Jesús Mauricio Andrade Guzmán (mandrade at seguridad dot unam dot mx)
- Eduardo González Martínez (egonzalez at seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
incidentes at seguridad.unam.mx
phishing at 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