UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−003

Oracle libera parches para múltiples Vulnerabilidades

Oracle ha publicado actualizaciones para varias vulnerabilidades en diferentes productos de la compañía. Los impactos de estas vulnerabilidades incluyen la ejecución de código arbitrario de forma remota, exposición de información sensible y negación de servicio.

Fecha de Liberación:	18 de Enero de 2007
Ultima Revisión:	19 de Enero de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Sistemas Afectados

Oracle Application Server 10g Release 1 (9.0.4),	==9.0.4.1
Oracle Application Server 10g Release 1 (9.0.4),	==9.0.4.2
Oracle Application Server 10g Release 1 (9.0.4),	==9.0.4.3
Oracle Application Server 10g Release 2	==10.1.2.0.0
Oracle Application Server 10g Release 2	==10.1.2.0.1
Oracle Application Server 10g Release 2	==10.1.2.0.2
Oracle Application Server 10g Release 2	==10.1.2.1.0
Oracle Application Server 10g Release 2	==10.1.2.2.0
Oracle Application Server 10g Release 3	==10.1.3.0.0
Oracle Application Server 10g Release 3	==10.1.3.1.0
Oracle Database 10g Release 1	==10.1.0.3
Oracle Database 10g Release 1	==10.1.0.4

Oracle Database 10g Release 1	==10.1.0.5
Oracle Database 10g Release 2	==10.2.0.1
Oracle Database 10g Release 2	==10.2.0.2
Oracle Database 10g Release 2	==10.2.0.3
Oracle Developer Suite	==10.1.2.0.2
Oracle Developer Suite	==6i
Oracle Developer Suite	==9.0.4.3
Oracle E−Business Suite Release 11i	==11.5.10 CU2
Oracle E−Business Suite Release 11i	==11.5.7
Oracle E−Business Suite Release 11i	==11.5.8
Oracle E−Business Suite Release 11i	==11.5.9
Oracle Enterprise Manager 10g Grid Control Release 1	==10.1.0.3
Oracle Enterprise Manager 10g Grid Control Release 1	==10.1.0.4
Oracle Enterprise Manager 10g Grid Control Release 1	==10.1.0.5
Oracle Enterprise Manager 10g Grid Control Release 2	==10.2.0.1
Oracle Identity Management 10g	==10.1.4.0.1
Oracle PeopleSoft Enterprise Tools	==8.22
Oracle PeopleSoft Enterprise Tools	**!=**8.47
Oracle PeopleSoft Enterprise Tools	==8.48
Oracle8i Database Release 3	==8.1.7.4
Oracle9i Application Server Release 1	==1.0.2.2
Oracle9i Application Server Release 2	==9.0.2.3
Oracle9i Database Server Release 1	==9.0.1.4
Oracle9i Database Server Release 1	==9.0.1.5
Oracle9i Database Server Release 1	==9.0.1.5 FIPS
Oracle9i Database Server Release 1	==9.2.0.7
Oracle9i Database Server Release 1	==9.2.0.8
Oracle9i Database Server Release 2	==9.2.0.5
Oracle9i Database Server Release 2	==9.2.0.6

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

Oracle ha publicado una actualización crítica – Enero 2007 que de acuerdo con la compañía esta actualización (CPU por sus siglas en inglés) contiene:

- 17 nuevas correcciones para el manejador de BD Oracle (Oracle atabase), uno de las cuales fue sólo para las instalaciones del cliente Oracle.
- 9 nuevas correcciones de seguridad para el servidor HTTP Oracle (Oracle HTTP Server)
- 12 nuevas correcciones de seguridad para el servidor de aplicaciones (Oracle Application Server).
- 7 nuevas correcciones para la suite de negocios (Oracle E−Business Suite).
- 6 nuevas correcciones de seguridad para el administrador empresarial (Oracle Enterprise Manager).
- 3 nuevas correcciones para el producto PeopleSoft Enterprise PeopleTools

Muchos productos Oracle incluyen o comparten código entre sí (ademas de otros componentes que son vulnerables). Por lo tanto, una vulnerabilidad podría afectar a múltiples productos y componentes de Oracle. Por ejemplo, en esta actualización crítica – enero 2007 no contiene ninguna corrección especificamente para el producto Oracle Collaboration Suite. Sin embargo , Oracle Collaboration Suite es afectado por las vulnerabilidades sobre Oracle Database y por las del Servidor de aplicaciones (Oracle Application Server), por lo que los sitios que ejecuten estas aplicaciones deben instalar las correcciones para dichas aplicaciones. Para ello se puede referir a las notas de actualización crítica enero 2007 para conocer detalles correspondientes a vulnerabilidades sobre productos y componentes de Oracle.

Para una lista publicada de vulnerabilidades que se cubren en la actualización crítica de Enero 2007 (CPU), por favor referirse al mapa público de vulnerabilidades.

En la alerta de seguridad Enero 2007 CPU no se asocia el identificador de la vulnerabilidad (ejemplo DB01) con otra información disponible, aún en el mapa público de vulnerabilidades, con algún documento de aviso o alerta.

II. **Impacto**

El impacto de estas vulnerabilidades varia dependiendo del producto o componente, y también sobre la configuración del sistema. Las consecuencia potenciales de estas, incluyen la ejecución comandos y de código arbitrario de forma remota, la exposición de información sensible, y la negación de servicio. Los componentes vulnerables podrían estar disponibles sin estar autenticados para atacantes remotos. Un atacante que comprometa un servidor de base de datos Oracle podría estar autorizado para obtener acceso a información confidencial o tomar el control completo de los sistemas o host remotos.

III. **Solución**

Aplicar los parches o actualizaciones especificadas dentro de las actualizaciones críticas − Enero 2007. Hay que tomar en cuenta que dichas notas de actualización solamente listan las nuevas vulnerabilidades corregidas.

Como se destaca en la actualización, algunos parches son acumulativos y otros no:

Los parches dentro de la actualización son acumulativos sobre los productos Oracle Database, el servidor aplicaciones (Oracle Application Server), el administrador empresarial Grid Control (Oracle Enterprise

Manager Grid Control), la suite de colaboración (Oracle Collaboration Suite),JD Edwards EnterpriseOne, JD Edwards OneWorld Tools, Portal de aplicaciones empresarial PeopleSoft (PeopleSoft Enterprise Portal Applications) y las herramientas empresariales de PeopleSoft Enterprise, en donde cada parche crítico contienen las correcciones de previas actualizaciones.

Para el Oracle E−Business Suite , las actualizaciones no son acumulativas, asi que los consumidores de este producto deben de referirse a las Actualizaciones Críticas de Parches previas en caso de querer aplicarla.

Las vulnerabilidades descritas en la Actualización Crítica de Parches Enero 2007 CPU podrían afectar a el motor de BD Oracle 10g Express Edition (Oracle Database XE). De acuerdo con oracle, esta versión de servidor esta basado sobre código de otra versión de servidor, la cual es Oracle 10g Release 2.

Se sabe que los parches de Oracle están documentados en las notas de pre−instalación y en los archivos readme de los parches. Se sugiere que se consulte estos documentos y se prueben antes de aplicarlos sobre sistemas en producción.

IV. Referencias

1. US−CERT Notas de Vulnerabilidad relacionadas a la Actualización Crítica de Parches – Enero 2007

   http://www.kb.cert.org/vuls/byid?searchview_jan_2007

2. Actualización Crítica de Parches – Enero 2007

   http://www.oracle.com/technology/deploy/security/critical−patch−updates/cpujan2007.html
3. Actualización crítica de Parches y alertas de seguridad

   http://www.oracle.com/technology/deploy/security/alerts.htm
4. Mapa de vulnerabilidades Map of Public Vulnerability to Advisory/Alert −

   http://www.oracle.com/technology/deploy/security/critical−patch−updates/public_vuln_to_advisory_m
5. Checklist de seguiridad para el motor BD Oracle (PDF) −

   http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf
6. Mejores prácticas para la implementación de Actualizaciones críticas (PDF)

   http://www.oracle.com/technology/deploy/security/pdf/cpu_whitepaper.pdf
7. Oracle Database 10g Express Edition

   http://www.oracle.com/technology/products/database/xe/index.html
8. Detalles sobre la Actualización crítica de Parches Enero 2007 −

   http://www.red−database−security.com/advisory/oracle_cpu_jan_2007.html

---

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

- Ricardo Carrillo Sanchez (rcarrillo at correo dot seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino 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