UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−015

Oracle libera las actualizaciones para múltiples vulnerabilidades.

Oracle ha liberado actualizaciones para tratar numerosas vulnerabilidades en diversos productos de Oracle. Los impactos de estas vulnerabilidades permiten la ejecución remota de código arbitrario, el acceso a la información, y la negación del servicio.

Fecha de Liberación: 19 de Abril de 2007

Ultima Revisión: 20 de Abril de 2007

Fuente: US−CERT

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas Afectados

- Oracle Database
- Oracle Application Server
- Oracle Secure Enterprise Search
- Oracle Enterprise Manager
- Oracle Collaboration Suite
- Ultra Search component
- Oracle E−Business Suite
- JD Edwards EnterpriseOne

II. Descripción

Oracle ha liberado el Critical Patch Update de Abril de 2007−. De acuerdo a Oracle, este CPU (Critical Patch Update) incluye:

- 13 Nuevas mejoras en la seguridad Oracle Databases
- 1 Nuevo arreglo de la seguridad de Oracle Secure Enterprise Search
- 1 Nuevo arreglo en la seguridad de Oracle Enterprise Manager
- 1 Nuevo arreglo de para la seguridad Oracle Workflow Cartridge
- 1 Nuevo arreglo en la seguridad de Ultra Search component

Muchos productos de Oracle incluyen o comparten código con otros productos y componentes vulnerables de Oracle.

Por lo tanto, una vulnerabilidad puede afectar múltiples productos y componentes Oracle. Dirijase a la CPU de abril del 2007 para mas detalles con respecto de las vulnerabilidades que afectan a los productos y componentes específicos de Oracle.

Hasta el 18 de abril de 2007, las actualizaciones para Oracle Vuln#s DB01 y DB03 no estaban disponibles.

Estas vulnerabilidades afectan la base de datos Oracle versión 9.2.0.8 únicamente en Windows

Para una lista completa de las vulnerabilidades conocidas, tratadas en la CPU de abril de 2007, diríjase al esquema de vulnerabilidades para Boletines/Alertas.

La CPU de abril de 2007 no asocia Vuln # ni los identificadores (e.g., DB01) a la información disponible, ni en el esquema de la vulnerabilidad que se pública en el documento.

Conforme estén disponibles más detalles sobre las vulnerabilidades y estrategias de mitigación, se actualizarán las notas individuales de vulnerabilidad.

III. Impacto

El impacto de estas vulnerabilidades varía dependiendo del producto, del componente, y de la configuración del sistema. Las consecuencias potenciales incluyen la ejecución remota de código o comandos ejecutados arbitrariamente, acceso a información sensible, y negación del servicio. Los componentes vulnerables pueden estar disponibles sin autenticación de los atacantes remotos.

Un atacante que compromete una base de datos de Oracle puede acceder a la información sensible o tomar el control completo del sistema.

IV. Solución

Aplicar las actualizaciones apropiadas o ponga las mas recientes según lo especificado en la CPU de abril del 2007. Observe que esta actualización crítica enumera solamente vulnerabilidades recientes corregidas.

Según lo observado en la actualización, algunos parches son acumulativos, otros no lo son:

Los parches para Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne, JD Edwards OneWorld Tools, PeopleSoft Enterprise Portal Applications y PeopleSoft Enterprise PeopleTools son acumulativos; Oracle E−Business Suite and Applications en las actualizaciones son acumulativos; cada CPU contiene los arreglos de las actualizaciones críticas anteriores.

Los parches para Oracle E−Business Suite and Applications no son acumulativos, de tal forma que los clientes de E−Business Suite and Applications deben referirse a los CPU anteriores para identificar correcciones previas que se quieran aplicar.

Las vulnerabilidades descritas en la CPU de abril de 2007 pueden afectar la Oracle Database 10g Express Edition (XE). Según Oracle, la base de datos XE se basa en el código de Oracle Database 10g Release 2. Las ediciones conocidas con los parches de Oracle se documentan en las notas de la preinstalación y los archivos de información del parche. Consulte por favor estos documentos y pongalos primero en sus sistemas de prueba antes de hacer el cambio a los sistemas de producción.

V. Referencias

- US−CERT Vulnerability Notes Related to Critical Patch Update April 2007
- Critical Patch Update − April 2007
- Critical Patch Updates and Security Alerts
- Map of Public Vulnerability to Advisory/Alert
- Oracle Database Security Checklist (PDF)
- Critical Patch Update Implementation Best Practices (PDF)
- Oracle Database 10g Express Edition
- Details Oracle Critical Patch Update April 2007

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

- Eduardo González Martínez (egonzalez 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