UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−004

Multiples Vulnerabilidades en Productos Oracle

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que varios productos Oracle y componentes están afectados con múltiples vulnerabilidades. El impacto de estas vulnerabilidades incluye la ejecución remota de código arbitrario, revelación de información y negación de servicio.

Fecha de Liberación:	18 de Enero de 2006
Ultima Revisión:	19 de Enero 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.F1
JD Edwards EnterpriseOne Tools, OneWorld Tools	==SP23_L1
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 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 Collaboration Suite 10g Release 1	==10.1.1
Oracle Collaboration Suite 10g Release 1	==10.1.2
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 E−Business Suite Release 11.0	==Todas
Oracle E−Business Suite Release 11i	>=11.5.1
Oracle E−Business Suite Release 11i	<=11.5.10 CU2
Oracle Enterprise Manager 10g Grid Control	==10.1.0.3
Oracle Enterprise Manager 10g Grid Control	==10.1.0.4
Oracle Workflow	>=11.5.1
Oracle Workflow	<=11.5.9.5
Oracle8i Database Release 3	==8.1.7.4
Oracle9i Collaboration Suite Release 2	==9.0.4.2
Oracle9i Database Release 2	==9.2.0.6
Oracle9i Database Release 2	==9.2.0.7
PeopleSoft Enterprise Portal	==8.4
PeopleSoft Enterprise Portal	==8.8
PeopleSoft Enterprise Portal	==8.9

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

Oracle ha liberado actualizaciones críticas de Enero de 2006. Estas actualizaciones son más de 80 vulnerabilidades en diferentes productos y componentes de Oracle.

La actualización crítica proporciona información sobre los componentes afectados, acceso y autorización requeridos, y el impacto de vulnerabilidades en la confidencialidad, integridad y disponibilidad de los datos. Para más información acerca de la actualización de seguridad, los clientes de Metalink deben dirigirse a la Nota 293956.1.

De acuerdo a Oracle, tres de las vulnerabilidades que fueron corregidas en la actualización crítica de Oracle de Enero de 2006 solamente afecta a los clientes de Base de Datos.

El UNAM−CERT recomienda que los sitios ejecutando Oracle revisen las actualizaciones críticas, apliquen las correcciones y tomen las medidas necesarias. El CERT está haciendo referencia a todas estas vulnerabilidades como VU#545804. Como

información adicional se publicarán las notas de la vulnerabilidad individualmente.

II. Impacto

El impacto de estas vulnerabilidades varía dependiendo del producto, componente y la configuración del sistema. Las consecuencias potenciales incluyen la ejecución de código o comandos arbitrarios, exposición de información sensible y denegación de servicio. Los componentes vulnerables están disponibles para los intrusos a través de redes remotas, con limitada o sin previa autorización. Un intruso que compromete una base de datos Oracle podría obtener acceso a información sensible.

III. Solución

Aplicar el parche

Aplicar los parches apropiados o actualizar con un parche especificado en la lista de actualizaciones críticas − Enero 2006. Note que en esta lista sólo vienen las nuevas correcciones. Las actualizaciones para versiones previas no están listadas.

Como se menciona en la actualización, algunos parches son acumulativos, mientras que otros no:

Los parches para Oracle Database, Oracle Application Server, Oracle Enterprise Manager Grid Control, Oracle Collaboration Suite, JD Edwards EnterpriseOne , OneWorld Tools, y el portal PeopleSoft Enterprise son acumulativos; cada parche crítico sucesivo contiene correcciones de actualizaciones anteriores.

Para el caso del Oracle E−Business Suite, no son acumulativos , así que para los clientes de este producto deben de hacer referencia a la lista de actualizaciones críticas para identificar correcciones previas por si quieren aplicarlas.

IV. Apéndice A. Información del fabricante

Oracle

Por favor ver la lista de actualizaciones críticas − Enero 2006 y las actualizaciones y alertas de seguridad.

V. Apéndice B. Referencias

- Lista de actualizaciones críticas − Enero 2006 − <http://www.oracle.com/technology/deploy/security/pdf/cpujan2006.html>
- Lista de actualizaciones críticas y alertas de seguridad− <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Nota MetaLink 293956.1 − <http://metalink.oracle.com/metalink/plsql/showdoc?db=Notgt;
- Vulnerabilidad US−CERT VU#545804 − <http://www.kb.cert.org/vuls/id/545804>
- Vulnerabilidad relacionada a Actualización Crítica − Enero 2006 − <http://www.kb.cert.org/vuls/byid?searchview_january_2006>
- Mapa público de la vulnerabilidad para avisos o alertas − <http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html>
- Checklist de seguridad para la base de datos Oracle (PDF) − <http://www.oracle.com/technology/deploy/security/pdf/twp_security_checklist_db_database.pdf>

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)
- Juan Lopez Morales (jlopez at correo dot seguridad dot unam dot mx)
- Ricardo Carrillo Sanchez (rcarrillo at correo dot 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