UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−016

Productos Oracle contienen múltiples vulnerabilidades

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

Fecha de Liberación:	19 de Octubre de 2005
Ultima Revisión:	20 de Octubre de 2005
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

JD Edwards EnterpriseOne, OneWorld XE	==8.94_Q1
JD Edwards EnterpriseOne, OneWorld XE	==8.95_B1
JD Edwards EnterpriseOne, OneWorld XE	==SP23_K1
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	==10.1.2.0.0
Oracle Application Server 10g Release 2	==10.1.2.0.1
Oracle Application Server 10g Release 2	==10.1.2.0.2
Oracle Clinical	==4.5.0
Oracle Clinical	==4.5.1
Oracle Collaboration Suite 10g Release 1	==10.1.1
	==10.1.0.3

Oracle Database Server 10g Release 1	
Oracle Database Server 10g Release 1	==10.1.0.4
Oracle Database Server 10g Release 1	==10.1.0.4.2
Oracle Developer Suite	==10.1.2.0
Oracle Developer Suite	==9.0.2.1
Oracle Developer Suite	==9.0.4.1
Oracle Developer Suite	==9.0.4.2
Oracle E−Business Suite Release 11.0	
Oracle E−Business Suite Release 11i	>=11.5.1
Oracle E−Business Suite Release 11i	<=11.5.10
Oracle E−Business Suite Release 11i	==11.5.10 CU2
Oracle Enterprise Manager 10g Database Control	==10.1.0.3
Oracle Enterprise Manager 10g Database Control	==10.1.0.4
Oracle Enterprise Manager 10g Grid Control	==10.1.0.3
Oracle Enterprise Manager 10g Grid Control	==10.1.0.4
Oracle Enterprise Manager Application Server Control	==9.0.4.1
Oracle Enterprise Manager Application Server Control	==9.0.4.2
Oracle Workflow	>=11.5.1
Oracle Workflow	<=11.5.9.5
Oracle8 Database Server Release 8.0.6	==8.0.6.3
Oracle8i Database Server 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 Application Server Release 2	==9.0.3.1
Oracle9i Collaboration Suite Release 2	==9.0.4.2
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
	==9.2.0.5

Oracle9i Database Server Release 2	
Oracle9i Database Server	==9.2.0.6
Oracle9i Database Server Release 2	
Oracle9i Database Server	==9.2.0.7
Release 2	
PeopleSoft CRM	>=8.81
PeopleSoft CRM	<=8.9
PeopleSoft Enterprise Tools	>=8.1
PeopleSoft Enterprise Tools	<=8.46.03

Riesgo

Crítico

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Descripción**

Oracle publicó una actualización crítica en este mes (Octubre del 2005). En donde se cubren más de 85 diferentes vulnerabilidades en diversos productos y componentes de Oracle.

La actualización de parches crítica provee información sobre los componentes afectados, acceso y autorización requerida, y el impacto de las vulnerabilidades sobre la confidencialidad, integridad y la disponibilidad de los datos. Para más información de los términos utilizados en dicha actualización, los clientes de Metalink deberían de hacer referencia a la Nota 293956.1 de Metalink.

De acuerdo a esta actualización crítica: "Las nuevas vulnerabilidades en la base de datos tratadas por esta actualización no afectan a las instalaciones sólo de cliente de la Base de datos Oracle (instalaciones que no se tienen el servidor de base de datos). Por lo tanto, no es necesario apicar esta actualización crítica para instalaciones sólo−cliente si ya ha sido aplidada una actualización crítica o alerta 68.

El UNAM−CERT recomienda que los sitios que estén ejecutando Oracle revisen la actualización crítica, que apliquen los parches, y tomen otras medidas o acciones apropiadas . UNAM−CERT está dando seguimiento a a todos estos temas bajo el nombre UNAM−CERT−2005−497.

II. **Impacto**

El impacto de estas vulnerabilidades varía dependiendo del producto, del componente, y, y la configuración del sistema operativo. Las consecuencias potenciales incluyen la ejecución de remota de código o comandos arbitrariamente, revelación de información y negación de servicio. Un atacante que comprometa un servidor de Bases de Datos Oracle podría obtener acceso a información confidencial o sensible.

III. **Solución**

Aplicar el parche

Aplicar los parches o actualizaciones apropiados como se especifica en la actualización crítica de Oracle del mes de Octubre del 2005. Debe notarse que esta actualización solo lista los problemas nuevos corregidos. Las actualizaciones para problemas conocidos anteriormente no están listados.

Soluciones temporales

Podría ser posible mitigar algunas vulnerabilidades si se deshabilita o quitan componentes innecesarios, restringiendo el acceso a la red, y restringiendo el acceso a archivos temporales.

La actualización crítica del mes de octubre 2005, sugiere deshabilitar el PSQL Manager para mitigar las vulnerabilidades en la herramienta PeopleSoft Enterprise y PeopleTools (PSE04)

IV. Apéndice A. Información del fabricante

Oracle

Por favor ver la actualización crítica del mes de octubre 2005 y las Actualizaciones Críticas y Alertas de Seguridad.

V. Apéndice B. Referencias

- Actualización crítica del mes de Octubre 2005 − <http://www.oracle.com/technology/deploy/security/pdf/cpuoct2005.html>
- 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=Not
- Nota de vulnerabilidad VU#210524 US−CERT − <http://www.kb.cert.org/vuls/id/210524>
- Notas de Vulnreabilidad relacionadas con la actualización crítica del mes de Octubre del 2005 US−CERT− <http://www.kb.cert.org/vuls/byid?searchview_october_2005>
- Mapa de Vulnerabilidad pública para avisos o alertas − http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html>
- SecurityFocus BugTraq − http://www.securityfocus.com/archive/1/413827/30/0/threaded>

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)

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