

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Boletín de Seguridad UNAM-CERT-2010-001

Actualizaciones de Oracle para múltiples vulnerabilidades

Los productos y componentes de Oracle son afectados por múltiples vulnerabilidades. Los impactos de estas vulnerabilidades incluyen ejecución remota de código arbitrario, revelación de información y denegación de servicio.

Fecha de Liberación: 12 de Enero de 2010

Última Revisión: 12 de Enero de 2010

Fuente: US-CERT

Riesgo

Crítico

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas Afectados

- ◆ Oracle Database 11g, versión 11.1.0.7
- ◆ Oracle Database 10g Release 2, versiones 10.2.0.3 y 10.2.0.4
- ◆ Oracle Database 10g, versión 10.1.0.5
- ◆ Oracle Database 9i Release 2, versiones 9.2.0.8 y 9.2.0.8DV
- ◆ Oracle Application Server 10g Release 3 (10.1.3), versiones 10.1.3.4.0, 10.1.3.5 y 10.1.3.5.1
- ◆ Oracle Application Server 10g Release 2 (10.1.2), versión 10.1.2.3.0
- ◆ Oracle Access Manager versiones 7.0.4.3 y 10.1.4.2
- ◆ Oracle E-Business Suite Release 12, versiones 12.0.4, 12.0.5, 12.0.6, 12.1.1 y 12.1.2
- ◆ Oracle E-Business Suite Release 11i, versión 11.5.10.2
- ◆ PeopleSoft Enterprise HCM (TAM), versiones 8.9 y 9.0
- ◆ Oracle WebLogic Server 10.0 a través de MP2, 10.3.0 y 10.3.1
- ◆ Oracle WebLogic Server 9.0 GA, 9.1 GA y 9.2 a través de 9.2 MP3
- ◆ Oracle WebLogic Server 8.1 a través de 8.1 SP6
- ◆ Oracle WebLogic Server 7.0 a través de 7.0 SP7

UNAM-CERT

- ◆ Oracle JRockit R27.6.5 y anteriores (JDK/JRE 6, 5 y 1.4.2)
- ◆ Primavera P6 Enterprise Project Portfolio Management 6.1, 6.2.1 y 7.0
- ◆ Primavera P6 Web Services 6.2.1, 7.0 y 7.0 SP1

II. Descripción

El Oracle Critical Patch Update Advisory Enero 2010, registró 24 vulnerabilidades en diversos productos y componentes de Oracle. El documento proporciona la información acerca de los componentes afectados, accesos y autorización requerida para explotación exitosa, y el impacto de las vulnerabilidades sobre la confidencialidad, integridad y disponibilidad de los datos.

Oracle tiene asociado identificadores CVE con los registros de vulnerabilidades en esta Actualización Crítica. Si requiere de detalles adicionales acerca de estas vulnerabilidades y sobre técnicas de corrección, mantendremos actualizada la Base de Datos de Notas de Vulnerabilidades.

III. Impacto

El impacto de estas vulnerabilidades varía dependiendo del producto, componente y configuración del sistema. Las consecuencias potenciales incluyen la ejecución de código arbitrario o comandos, revelación de información y denegación de servicio. Los componentes vulnerables pueden estar disponibles a atacantes remotos no autenticados. Un atacante que comprometa una base de datos Oracle puede ganar acceso a información sensible.

IV. Solución

Aplicar los parches o actualizaciones apropiadas como se especifica en el Oracle Critical Patch Update Advisory Enero 2010. Tenga en cuenta que este documento sólo muestra los problemas corregidos recientemente. Las actualizaciones de parches de problemas anteriores no aparecen.

V. Referencias

- ◆ Oracle Patch Update Advisory Enero 2010 -
<http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpujan2010.html>
- ◆ Actualizaciones Críticas y Alertas de Seguridad -
<http://www.oracle.com/technology/deploy/security/alerts.htm>
- ◆ Mapa de Vulnerabilidades Públicas/Alerta -
[http://www.oracle.com/technology/deploy/security/critical-patch-updates/public_vuln to advisory m](http://www.oracle.com/technology/deploy/security/critical-patch-updates/public_vuln_to_advisory_m)

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

- Carmina Cecilia Espinosa Madrigal (cespinosa 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
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 47