UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2009−010

Actualizaciones de Oracle para Múltiples Vulnerabilidades

Los productos y componentes Oracle son afectados por múltiples vulnerabilidades. El impacto de estas vulnerabilidades incluye la ejecución remota de código arbitrario, acceso a información y denegación de servicio.

Fecha de Liberación: 15 de Abril de 2009

Ultima Revisión: 14 de Mayo de 2009

Fuente: US−CERT

Sistemas Afectados

Linux	**Oracle9i Database Release 2**	<9.2.0.8
Linux	**Oracle9i Database Release 2**	<9.2.0.8DV
Linux	**Oracle Application Server 10g Release 2**	<10.1.2
Linux	**Oracle Application Server 10g Release 2**	<10.1.2.3.0
Linux	**Oracle AquaLogic Data Services Platform (antes BEA ALDSP)**	<3.0
Linux	**Oracle AquaLogic Data Services Platform (antes BEA ALDSP)**	<3.0.1
Linux	**Oracle AquaLogic Data Services Platform (antes BEA ALDSP)**	<3.2
Linux	**Oracle BI Publisher**	<10.1.3.3.0
Linux	**Oracle BI Publisher**	<10.1.3.3.1
Linux	**Oracle BI Publisher**	<10.1.3.3.2
Linux	**Oracle BI Publisher**	<10.1.3.3.3
Linux	**Oracle BI Publisher**	<10.1.3.3.4
Linux	**Oracle Database 10g**	<10.1.0.5

Linux	**Oracle Database 10g Release 2**	<10.2.0.3
Linux	**Oracle Database 10g Release 2**	<10.2.0.4
Linux	**Oracle Database 11g**	<11.1.0.6,
Linux	**Oracle Database 11g**	<11.1.0.7
Linux	**Oracle Data Service Integrator**	<10.3.0
Linux	**Oracle E−Business Suite Release 11i**	<11.5.10.2
Linux	**Oracle E−Business Suite Release 12**	<12.0.6
Linux	**Oracle JRockit (antes BEA JRockit)**	<JDK/JRE 1.4.2
Linux	**Oracle JRockit (antes BEA JRockit)**	<JDK/JRE 5
Linux	**Oracle JRockit (antes BEA JRockit)**	<JDK/JRE 6
Linux	**Oracle JRockit (antes BEA JRockit)**	<R27.6.2
Linux	**Oracle Outside en SDK HTML Export**	<8.2.2
Linux	**Oracle Outside en SDK HTML Export**	<8.3.0
Linux	**Oracle WebLogic Server 10.3**	<−−
Linux	**Oracle WebLogic Server 7.0 con SP7**	<−−
Linux	**Oracle WebLogic Server 8.1 con SP6**	<−−
Linux	**Oracle WebLogic Server 9.0 GA**	<−−
Linux	**Oracle WebLogic Server 9.1 GA**	<−−
Linux	**Oracle WebLogic Server 9.2 con MP3**	<−−
Linux	**Oracle XML Publisher**	<10.1.3.2
Linux	**Oracle XML Publisher**	<10.1.3.2.1
Linux	**Oracle XML Publisher**	<5.6.2
Linux	**PeopleSoft Enterprise HRMS**	<8.9
Linux	**PeopleSoft Enterprise HRMS**	<9.0
Linux	**PeopleSoft Enterprise PeopleTools**	<8.49

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Acceso remoto al sistema

I. **Descripción**

El Aviso sobre el Parche de Actualización Crítica de Oracle – de Abril del 2009 presenta 43 vulnerabilidades en varios productos y componentes de Oracle. El documento proporciona la información sobre componentes afectados, acceso y autorización requerida para el éxito de la explotación, y el impacto de las vulnerabilidades sobre la confidencialidad de datos, la integridad, y la disponibilidad.

Oracle ha asociado identificadores CVE con las vulnerabilidades presentadas en este Parche de Actualización Crítica. Adicionalmente se mencionan significativos detalles sobre vulnerabilidades y técnicas disponibles para remediarlas, en la actualización de las Notas de Vulnerabilidades de la Base de datos.

II. **Impacto**

El impacto de estas vulnerabilidades varía dependiendo del producto, componente y configuración del sistema. Consecuencias potenciales incluyen la ejecución de código arbitrario o comandos, descubrimiento de información y denegación de servicio. Componentes vulnerables pueden estar disponibles para atacantes remotos sin autenticación.

Un atacante que compromete una base de datos de Oracle puede ser capaz de tener acceso a información sensible.

III. **Solución**

Aplique los parches apropiados o la mejora como se especifica en el Aviso sobre el Parche de Actualización Crítica de Oracle –Abril del 2009. Note que este documento sólo muestra los nuevos problemas recién corregidas. Las actualizaciones a parches para problemas conocidos previamente no son listadas.

IV. **Referencias**

* Aviso sobre el Parche de Actualización Crítica de Oracle –Abril del 2009

http://www.oracle.com/technology/deploy/security/critical−patch−updates/cpuapr2009.html

* Parches de Actualizaciones Críticas y Alertas de Seguridad

http://www.oracle.com/technology/deploy/security/alerts.htm

* Mapa de vulnerabilidades publicas para Consulta/Alertas

http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html

_____

La versión más reciente de este documento se puede encontrar en:

http://www.us−cert.gov/cas/techalerts/TA09−105A.html

Material

Documento: excel.pdf (304678kb)

Video (Descarga): Excel.flv (1427kb)

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

- Tania Montero (tmontero at seguridad dot unam dot mx)
- José Roberto Sánchez Soledad (rsanchez 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