Boletin de Seguridad UNAM-CERT-2011-008 Actualizaciones de Oracle para múltiples vulnerabilidades

Los productos y componentes Oracle mencionados anteriormente, son afectados por múltiples vulnerabilidades. Los impactos de estas vulnerabilidades incluyen la ejecución remota de código arbitrario, divulgación de información y negación de servicio.

- **Fecha de Liberación:** 20-Jul-2011
- **Ultima Revisión:** 20-Jul-2011
- **Fuente:** US-CERT
- **Riesgo** Crítico
- **Problema de Vulnerabilidad** Remoto
- **Tipo de Vulnerabilidad** Ejecución remota de código y negación de servicio

Sistemas Afectados

Oracle Agile Technology Platform	==	9.3.0.3
Oracle Agile Technology Platform	==	9.3.1.1
Oracle Application Server 10g Release 2	==	10.1.2.3.0
Oracle Application Server 10g Release 3	==	10.1.3.5.0
Oracle Business Intelligence Enterprise Edition	==	10.1.3.4.1
Oracle Business Intelligence Enterprise Edition	==	11.1.1.3
Oracle Database 10g Release 1	==	10.1.0.5
Oracle Database 10g Release 2	==	10.2.0.3
Oracle Database 10g Release 2	==	10.2.0.4
Oracle Database 10g Release 2	==	10.2.0.5
Oracle Database 11g Release 1	==	11.1.0.7
Oracle Database 11g Release 2	==	11.2.0.1
Oracle Database 11g Release 2	==	11.2.0.2
Oracle E-Business Suite Release 11i	==	11.5.10.2
Oracle E-Business Suite Release 12	==	12.0.4
Oracle E-Business Suite Release 12	==	12.0.6
Oracle E-Business Suite Release 12	==	12.1.1
Oracle E-Business Suite Release 12	==	12.1.2
Oracle E-Business Suite Release 12	==	12.1.3
Oracle Enterprise Manager 10g Grid Control Release 1	==	10.1.0.6
Oracle Enterprise Manager 10g Grid Control Release 1	==	11.1.0.1
Oracle Enterprise Manager 10g Grid Control Release 2	==	10.2.0.5
Oracle Fusion Middleware 11g Release 1	==	11.1.1.3.0
Oracle Fusion Middleware 11g Release 1	==	11.1.1.4.0
Oracle Fusion Middleware 11g Release 1	==	11.1.1.5.0
Oracle Identity Management 10g	==	10.1.4.0.1

Oracle Identity Management 10g	==	10.1.4.3
Oracle JRockit	<	R27.6.9
Oracle JRockit	<	R28.1.3
Oracle Outside In Technology	==	8.3.2.0
Oracle Outside In Technology	==	8.3.5.0
Oracle PeopleSoft Enterprise FIN	==	9.0
Oracle PeopleSoft Enterprise FIN	==	9.1
Oracle PeopleSoft Enterprise FMS	==	9.0
Oracle PeopleSoft Enterprise FMS	==	9.1
Oracle PeopleSoft Enterprise FSCM	==	9.0
Oracle PeopleSoft Enterprise FSCM	<	9.1
Oracle PeopleSoft Enterprise HRMS	==	8.9
Oracle PeopleSoft Enterprise HRMS	==	9.0
Oracle PeopleSoft Enterprise HRMS	==	9.1
Oracle PeopleSoft Enterprise PeopleTools	>=	8.49
Oracle PeopleSoft Enterprise SCM	==	9.0
Oracle PeopleSoft Enterprise SCM	==	9.1
Oracle Secure Backup	==	10.3.0.3

1. Descripción

El Boletín de Actualización para Parches Críticos de Oracle - Julio 2011 presenta 78 vulnerabilidades en varios productos y componentes de Oracle. El boletín proporciona información acerca de los componentes afectados, el acceso y la autorización requerida para la explotación satisfactoria y el impacto de las vulnerabilidades en la confidencialidad, integridad y disponibilidad de la información.

Oracle ha asociado identificadores CVE con las vulnerabilidades contempladas en el Boletín de Actualización para Parches Críticos de Oracle - Julio 2011. Más detalles acerca de alguna vulnerabilidad están disponibles en la Nota de Vulnerabilidad de US-CERT VU#103425.

2. Impacto

El impacto de estas vulnerabilidades varía dependiendo del producto, el componente y la configuración del sistema. Consecuencias potenciales incluyen la ejecución de código arbitrario o comandos, revelación de información y negación de servicio. Componentes vulnerables pueden estar disponibles para atacantes externos y no autenticados. Un atacante que comprometa una base de datos Oracle puede ser capaz de acceder a información sensible.

3. Solución

Aplicar los parches apropiados o actualizar como se especifica en el Boletín de Actualización para Parches Críticos de Oracle - Julio 2011. Tener en cuenta que este documento sólo menciona los problemas corregidos recientemente. Las actualizaciones de parches para problemas anteriores, no son mencionadas.

La Subdirección de Seguridad de la Información/UNAM-CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Iván Alvarado (ialvarado 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
Subdirección de Seguridad de la Información

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