Alerta de Seguridad Informática (9VSA-00019-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

Notificación

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática comparte una información publicada por Oracle referente a parches de actualización críticos para la mitigación de diversas vulnerabilidades que afectan a sus productos. Esta actualización de parches críticos contiene 319 nuevas correcciones de seguridad.

Vulnerabilidad

Esta actualización de parches críticos contiene 319 nuevas correcciones de seguridad en las familias de productos que se enumeran a continuación.

Impacto

Dependiendo del software afectado Oracle ha generado una matriz de riesgos que puede ser consultada en el link que se encuentra en la sección enlaces de este documento.

Productos Afectados

- Oracle Database Server
- Oracle Global Lifecycle Management
- Oracle Berkeley DB
- Oracle Communications Applications
- Oracle Construction and Engineering Suite
- Oracle E-Business Suite
- Oracle Enterprise Manager Products Suite
- Oracle Financial Services Applications
- Oracle Food and Beverage Applications
- Oracle Fusion Middleware
- Oracle Hospitality Applications
- Oracle Hyperion
- Oracle Insurance Applications
- Oracle Java SE
- Oracle GraalVM
- Oracle JD Edwards Products
- Oracle MySQL
- Oracle PeopleSoft Products
- Oracle Retail Applications
- Oracle Siebel CRM
- Oracle Sun Systems Products Suite
- Oracle Supply Chain Products Suite
- Oracle Support Tools
- Oracle Utilities Applications
- Oracle Virtualization

Mitigación

Se recomienda encarecidamente mantener actualizados a la última versión los software utilizados, en el caso de Oracle se necesita contar con las credenciales de soporte vigentes para poder realizar la descarga de parches e información adicional asociada al parche.

Enlaces

https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.07.17
18:51:05 -04'00'