DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 017**	**Fecha: 19-01-2023** **Página 5 de 12**

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Oracle publica aviso de actualización de Parche Crítico (enero 2023) que afecta a varias familias de sus productos		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Oracle ha publicado una actualización **CRÍTICA** con parches para corregir vulnerabilidades que afectan a múltiples productos. Esta actualización de parche crítico contiene 327 nuevos parches de seguridad en las familias de productos de Oracle. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante realizar actividades maliciosas en las familias de productos de Oracle.

2. **Detalles:**

- Una actualización de parche crítico es una colección de parches para múltiples vulnerabilidades de seguridad. Estos parches abordan las vulnerabilidades en el código de Oracle y en los componentes de terceros incluidos en los productos de Oracle. Estos parches suelen ser acumulativos, pero cada aviso describe solo los parches de seguridad agregados desde el Aviso de actualización de parche crítico anterior. Por lo tanto, los avisos de actualización de parches críticos anteriores deben revisarse para obtener información sobre los parches de seguridad publicados anteriormente.
- Esta actualización de parche crítico contiene 327 nuevos parches de seguridad en las familias de productos de Oracle. Tenga en cuenta que una nota de MOS que resume el contenido de esta actualización de parche crítico y otras actividades de Oracle Software Security Assurance se encuentra en: Actualización de parche crítico de enero de 2023: Resumen ejecutivo y análisis .

3. **Productos afectados:**

- Big Data Spatial y Graph, versiones anteriores a 21.4.3, anteriores a 23.1.0;
- Plataforma basada en Enterprise Manager, versiones 13.4.0.0, 13.5.0.0;
- Enterprise Manager Ops Center, versión 12.4.0.0;
- Servidores Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S, versiones anteriores a XCP2411, anteriores a XCP3111, anteriores a XCP4011;
- GoldenGate Stream Analytics, versiones anteriores a 19.1.0.0.8;
- GoldenGate Veridata, versiones anteriores a 12.2.1.4.220831;
- JD Edwards EnterpriseOne Orchestrator, versiones anteriores a 9.2.7.2;
- JD Edwards EnterpriseOne Tools, versiones anteriores a 9.2.7.2;
- Motor de gestión en la nube, versión 22.1.0.0.0;
- Management Pack para Oracle GoldenGate, versiones anteriores a 12.2.1.2.221115;
- Herramientas y bibliotecas comunes de Middleware, versiones 12.2.1.4.0, 14.1.1.0.0;
- MySQL Cluster, versiones 7.4.38 y anteriores, 7.5.28 y anteriores, 7.6.24 y anteriores, 8.0.31 y anteriores;
- MySQL Connectors, versiones 8.0.31 y anteriores;
- MySQL Enterprise Monitor, versiones 8.0.32 y anteriores;
- MySQL Server, versiones 5.7.40 y anteriores, 8.0.31 y anteriores;
- MySQL Shell, versiones 8.0.31 y anteriores;
- MySQL Workbench, versiones 8.0.31 y anteriores;
- Administrador de acceso de Oracle, versión 12.2.1.4.0;
- Oracle Agile PLM, versión 9.3.6;
- Oracle AutoVue, versiones anteriores a 21.0.2.6;
- Oracle Banking Enterprise Default Management, versiones 2.6.2, 2.7.0, 2.7.1, 2.12.0;

- Oracle Banking Loans Servicing, versiones 2.8.0, 2.12.0;
- Oracle Banking Party Management, versión 2.7.0;
- Oracle Banking Platform, versiones 2.6.2, 2.7.1, 2.9.0, 2.12.0;
- Oracle BI Publisher, versiones 5.9.0.0.0, 6.4.0.0.0, 12.2.1.4.0;
- Oracle Business Intelligence Enterprise Edition, versiones 5.9.0.0.0, 6.4.0.0.0;
- Oracle Coherence, versiones 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
- Búsqueda guiada de Oracle Commerce, versión 11.3.2;
- Ver lista completa aquí.

4. Solución:

- Oracle recomienda aplicar los parches de actualización de parche crítico, es posible reducir el riesgo de un ataque exitoso al bloquear los protocolos de red requeridos por un ataque;
- Para los ataques que requieren ciertos privilegios o acceso a ciertos paquetes, eliminar los privilegios o la capacidad de acceder a los paquetes de los usuarios que no los necesitan puede ayudar a reducir el riesgo de un ataque exitoso. Ambos enfoques pueden interrumpir la funcionalidad de la aplicación, por lo que Oracle recomienda encarecidamente que los clientes prueben los cambios en sistemas que no sean de producción. Ningún enfoque debe considerarse una solución a largo plazo, ya que ninguno corrige el problema subyacente.

Fuentes de información	▪ hxxps://www.oracle.com/security-alerts/cpujan2023.html ▪ hxxps://www.oracle.com/security-alerts/cpujan2023verbose.html ▪ hxxps://support.oracle.com/rs?type=doc&id=2834534.1 ▪ hxxps://www.oracle.com/security-alerts ▪ hxxps://www.oracle.com/security-alerts/advisorymatrixglossary.html