BOLETÍN DE ALERTA

Boletín Nro.: 2020-23

Fecha de publicación: 17/07/2020

Tema: Actualizaciones de seguridad para productos de Oracle abordan 443 vulnerabilidades catalogadas como críticas, altas, medias y bajas.

Sistemas afectados:

- Oracle Retail Applications
- Oracle Database Server
- Oracle GoldenGate
- Oracle Communications Applications
- Oracle Construction and Engineering
- Oracle E-Business Suite
- Oracle Enterprise Manager
- Oracle Financial Services Applications
- Oracle Fusion Middleware
- Oracle GraalVM
- Oracle Health Sciences Applications
- Oracle Hospitality Applications
- Oracle iLearning
- Oracle Insurance Applications
- Oracle Java SE
- Oracle JD Edwards
- Oracle MySQL
- Oracle PeopleSoft
- Oracle Siebel CRM
- Oracle Supply Chain
- Oracle Systems
- Oracle Utilities Applications
- Oracle Virtualization

Descripción:

Recientemente Oracle lanzó actualizaciones de seguridad para múltiples productos, donde abordan un total de 433 vulnerabilidades de riesgo **crítico**, **alto**, **medio** y **bajo**.

A continuación, se detallan brevemente las vulnerabilidades **críticas** más resaltantes.

Se identificaron vulnerabilidades que permitirían a un atacante no autenticado y con acceso a la red, **comprometer** el producto afectado:

- El CVE-2020-14705, afecta a **Oracle GoldenGate** en versiones anteriores a la **19.1.0.0.0.**
- Los CVE-2020-14701 y CVE-2020-14606, afectan a la interfaz de usuario de los productos **Oracle SD-WAN Aware** y **Edge** en **versiones 8.2** y **9.0.**
- Los CVE-2019-2729 y CVE-2019-2904, afectan a los componentes **Oracle WebLogic Server y JDeveloper** de **Oracle Communications Network Integrity** versiones **7.3.2-7.3.6**.
- Los CVE-2018-11776 y CVE-2019-0227, afectan a **Enterprise Manager Base 12.1.0.5, 13.3.0.0, 13.4.0.0; y Enterprise Manager** para **Fusion Middleware** versión **12.1.0.5**.
- El CVE-2020-14569, afecta a **Oracle FLEXCUBE Investor Servicing** versión **2.1.0, 12.3.0, 12.4.0, 14.0.0 y 14.1.0.**
- Los CVE-2020-14625, CVE-2020-14644, CVE-2020-14645 y CVE-2020-14687, afectan al núcleo de **Oracle WebLogic Server** en versiones **10.3.6.0.0**, **12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0.**
- El CVE-2020-14583, afecta al componente Java SE de **Oracle GraalVM Enterprise Edition** versiones **19.3.2 y 20.1.0.**
- El CVE-2020-2555, afecta a **Oracle Coherence** en versiones **3.7.1.0, 12.1.3.0.0, 12.2.1.3.0 y 12.2.1.4.0.**

Además, fueron abordadas vulnerabilidades de **ejecución remota de código:**

- El CVE-2020-1938, afecta a **Oracle Communications Element Manager 8.1.1, 8.2.0 y 8.2.1.**
- El CVE-2017-5645, afecta al componente **Apache Ant** de **Primavera Gateway** versiones **16.2.0-16.2.11 y 17.12.0-17.12.7.**

- El CVE-2017-15708, afecta a la interfaz de usuario (**Apache Synapse**) de **Oracle Financial Services Market Risk Measurement and Management** versiones **8.0.6, 8.0.8.**
- El CVE-2016-4000, afecta al componente **jython** de **Oracle Rapid Planning 12.1 y 12.2.**
- El CVE-2016-1000031, afecta al componente **MapViewer(Apache Commons FileUpload)** en versiones **12.2.0.1, 18c y 19c**; y **Oracle Communications Contacts Server 8.0.0.4.0.**

Por otro lado, se identificaron vulnerabilidades que permitirían a un atacante obtener **información** confidencial y/o potencialmente útil para realizar otros ataques. El CVE-2018-11058, afecta a **Communications Analytics** versión 12.1.1 y a **Oracle WebLogic Server** en versiones 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 y 12.2.1.4.0. Mientras que el CVE-2020-7060, afecta a **Oracle Communications Diameter Signaling Router (DSR) 8.0-8.4.** Y finalmente, el CVE-2020-1945, afecta a los productos:

- Primavera Unifier 16.1, 16.2, 17.7-17.12, 18.8 y 19.12;
- Oracle Communications Order and Service Management 7.3, 7.4;
- Oracle Communications MetaSolv Solution 6.3.0;
- Oracle Rapid Planning 12.1, 12.2;
- Oracle Retail, las **versiones específicas** afectadas pueden ser visualizadas en el siguiente **enlace** y
- Enterprise Manager Ops Center 12.4.0.0.

Vulnerabilidades de **XXE (XML External Entity)**. Las cuales podrían permitir a un atacante obtener datos confidenciales, realizar ataques de denegación de servicio **(DoS)**, falsificar solicitudes del lado del servidor, escanear puertos, y ejecutar código remoto en el sistema afectado:

- El CVE-2020-10683, afecta al componente **dom4j** de **Primavera P6 Enterprise Project Portfolio Management** en versiones **16.1.0.0-16.2.20.1, 17.1.0.0-17.12.17.1, 18.1.0.0-18.8.19 y 19.12.0-19.12.6.**

- El CVE-2019-13990, afecta a:
    - Oracle Communications IP Service Activator versiones 7.3.0 y 7.4.0;
    - Oracle Banking Payments versiones 14.1.0-14.4.0;
    - Oracle FLEXCUBE Investor Servicing versiones 12.1.0, 12.3.0, 12.4.0, 14.0.0 y 14.1.0 ;
    - Oracle FLEXCUBE Private Banking versiones 12.0.0, 12.1.0;
    - Customer Management and Segmentation Foundation 18.0;
    - Oracle Retail Integration Bus versiones 15.0, 16.0 y
    - Oracle Retail Xstore Point of Service 15.0, 16.0, 17.0, 18.0, 19.0.

Por otro lado el CVE-2020-11656, trata de una vulnerabilidad de use-after-free que afecta a los productos **Oracle Communications Network Charging and Control** 6.0.1 y 12.0.0-12.0.3; y **Oracle ZFS Storage Appliance Kit 8.8.**

Mientras que el CVE-2018-17196, trata de una vulnerabilidad que permitiría a un atacante sobrepasar restricciones y afecta al cliente Apache Kafka de **Primavera P6 Enterprise Project Portfolio Management** versiones **19.12.0-19.12.6**.

Además se identificaron vulnerabilidades que ser explotadas exitosamente permitirían a un atacante realizar modificaciones y visualizar datos confidenciales en el sistema afectado. El CVE-2020-14598, afecta a **Oracle CRM Gateway** para dispositivos móviles en versiones **12.1.1-12.1.3;** el CVE-2020-14599 afecta **Oracle Marketing en** versiones **12.1.1-12.1.3, 12.2.3-12.2.9** y el CVE-2020-14658 afecta a **Oracle Trade Management** en versiones **12.1.1-12.1.3, 12.2.3-12.2.9.**

Múltiples fallos de **Polymorphic Typing,** que permitirían a un atacante ejecutar **payloads** maliciosos. El CVE-2019-17531, afecta al framework de seguridad de **Oracle WebCenter Portal 12.2.1.3.0, 12.2.1.4.0**. Los CVE-2019-12086 y CVE-2019-16943, afectan al componente **jackson-databind** de los siguientes productos:

- Customer Management and Segmentation Foundation 18.0,
- Oracle Retail Merchandising System 15.0.3, 16.0.2 y 16.0.3;

- Oracle Retail Sales Audit 14.1.
- Siebel Engineering - Installer & Deployment versiones 2.20.5 y anteriores
- Siebel UI Framework versiones 20.5 y anteriores

El CVE-2019-17560, trata de una vulnerabilidad de **inyección de código** y afecta al componente Apache Netbeans de **Oracle GraalVM Enterprise Edition** versiones **19.3.2 y 20.1.0.**

El CVE-2016-5019, trata de una vulnerabilidad de **deserialización insegura**. La explotación exitosa podría permitir a un atacante realizar ataques de denegación de servicios (DoS) o ejecutar código remoto. Este fallo afecta al componente Apache Trinidad de **Oracle Rapid Planning** versiones **12.1 y 12.2.**

El CVE-2020-9546, se da debido a que el componente **jackson-databind** no maneja correctamente la interacción entre los dispositivos de serialización y afecta a los productos:

- Oracle Communications Contacts Server versión 8.0.0.4.0;
- Oracle Communications Evolved Communications Application Server 7.1;
- Primavera Unifier 16.1, 16.2, 17.7-17.12, 18.8 y 19.12;
- Oracle Communications Instant Messaging Server 10.0.1.4.0;
- Oracle Communications Network Charging and Control versiones 6.0.1, 12.0.0-12.0.3;
- Enterprise Manager Base Platform versiones 13.3.0.0, 13.4.0.0;
- Oracle Banking Platform versiones 2.4.0-2.9.0;
- Oracle WebLogic Server versiones 12.2.1.3.0, 12.2.1.4.0;
- JD Edwards EnterpriseOne Orchestrator versiones anteriores a la 9.2.4.2 y
- Oracle Retail Xstore Point of Service versiones 15.0, 16.0, 17.0, 18.0, 19.0.

Finalmente, se abordaron fallos de **riesgo alto**, algunos de ellos son:

Vulnerabilidades que permitirían a un atacante tomar control del sistema afectado en **Oracle VM VirtualBox** (CVE-2020-14628, CVE-2020-14646, CVE-2020-14647, CVE-2020-14649), **Java SE** (CVE-2020-14664, CVE-2020-14583) y **Oracle Database Server** (CVE-2020-2968) . Vulnerabilidades de **denegación de servicios (DoS)** en **MySQL Server** , **MySQL Connector** (CVE-2020-1967) y **Java SE** (CVE-2020-14562). Más detalles, sobre todas las

vulnerabilidades abordadas pueden ser visualizados en el **aviso de seguridad oficial de Oracle**.

Impacto:

Estas vulnerabilidades podrían permitir a un atacante:

- Ejecutar código,
- Ejecutar ataques de **denegación de servicios (DoS)**,
- Comprometer el producto afectado y
- Obtener **información confidencial** y/o potencialmente **útil** para realizar otros ataques.

Solución y prevención:

Aplicar las actualizaciones de seguridad para los productos afectados, desde el apartado "**Patch Availability Document**" del **boletín de seguridad** publicado por **Oracle**.

Información adicional:

- https://www.oracle.com/security-alerts/cpujul2020.html
- https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/actualizaciones-criticas-oracle-julio-2020
- https://us-cert.cisa.gov/ncas/current-activity/2020/07/14/oracle-releases-july-2020-security-bulletin