cyber zaintza
BASQUE CYBERSECURITY AGENCY

# Actualización de seguridad de Oracle-Abril 2024

**TLP: CLEAR**

www.ciberseguridad.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

## TABLA DE CONTENIDO

## Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que la Agencia de Ciberseguridad Vasca considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso la Agencia de Ciberseguridad Vasca puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de la Agencia de Ciberseguridad Vasca como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de la Agencia de Ciberseguridad Vasca. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

## Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

## 1. Resumen ejecutivo

**Oracle** ha publicado su boletín trimestral de actualizaciones de seguridad, que aborda **441 correcciones** en una amplia variedad de productos. La mayoría de estos fallos permiten a un atacante remoto comprometer la **integridad**, **confidencialidad** y **disponibilidad** de los sistemas afectados, lo que podría dar lugar a la pérdida de datos y la interrupción de los servicios.

Estas vulnerabilidades tienen impacto en los siguientes componentes:

- Oracle Autonomous Health Framework.
- Oracle Management Cloud Engine.
- Oracle MySQL.
- Oracle Global Lifecycle Management.
- Oracle Fusión Middleware.
- Oracle Supply Chain Componentes.
- Oracle Enterprise Manager.
- Oracle Banking Deposits and Lines of Credit Servicing.
- Oracle Banking Platform.
- Oracle Analytics.
- Oracle Commerce.
- Oracle Communications Billing and Revenue Management.
- Oracle Communications BRM - Elastic Charging Engine.
- Oracle Communications Cloud Native Core Binding Support Function.
- Oracle Communications Cloud Native Core Console.
- Oracle Communications Cloud Native Core Network Data Analytics Function.
- Oracle Communications Cloud Native Core Network Exposure Function.
- Oracle Communications Cloud Native Core Network Function Cloud Native Environment.
- Oracle Communications Cloud Native Core Network Repository Function.
- Oracle Communications Cloud Native Core Network Slice Selection Function.
- Oracle Communications Cloud Native Core Policy.
- Oracle Communications Cloud Native Core Security Edge Protection Proxy.
- Oracle Communications Cloud Native Core Service Communication Proxy.
- Oracle Communications Cloud Native Core Unified Data Repository.
- Oracle Communications Diameter Signaling Router.
- Oracle Communications Element Manager.
- Oracle Communications Fraud Monitor.
- Oracle Communications Network Integrity.

- Oracle Communications Offline Mediation Controller.
- Oracle Communications Operations Monitor.
- Oracle Communications Service Catalog and Design.
- Oracle Communications Session Report Manager.
- Oracle Communications Unified Inventory Management.
- Oracle Communications User Data Repository.
- Oracle Communications WebRTC Session Controller.
- Oracle Insurance Applications.
- Oracle E-Business Suite.
- Oracle Financial Services Revenue Management and Billing.
- Oracle Java SE.
- Oracle HealthCare Applications.
- Oracle Hospitality Cruise Shipboard Property Management System.
- Oracle Hospitality Simphony.
- Oracle Enterprise Performance Management.
- Oracle Health Sciences.
- Oracle Retail Applications.
- Oracle SD-WAN Edge.
- Oracle Utilities Applications.
- Oracle Support Tools.
- Oracle PeopleSoft.
- Oracle Construction and Engineering Suite.
- Oracle Siebel.

Para prevenir estas y otras vulnerabilidades, se recomienda tener siempre los sistemas y aplicaciones actualizadas a la última versión disponible.

## 2. Recursos afectado

Las actualizaciones de seguridad del mes de abril de 2024 están asociadas a vulnerabilidades que afectan a los siguientes componentes:

| Componenteos y versiones afectadas | Documento de disponibilidad de actualizaciones |
|---|---|
| Autonomous Health Framework, versiones:<br>anteriores a 23.11.1 y 24.2 | Oracle Autonomous Health Framework |
| Management Cloud Engine, versión 24.1.0.0.0 | Management Cloud Engine |
| MySQL Cluster, versiones:<br>• 7.5.33 y anterior<br>• 7.6.29 y anterior<br>• 8.0.36 y anterior<br>• 8.2.0 y anterior<br>• 8.3.0 y anterior | MySQL |
| MySQL Connectors, version 8.3.0 y anterior | MySQL |
| MySQL Enterprise Backup, versiones:<br>• 8.0.36 y anterior<br>• 8.3.0 y anterior | MySQL |
| MySQL Enterprise Monitor, version 8.0.37 y anterior | MySQL |
| MySQL Server, versiones:<br>• 8.0.36 y anterior<br>• 8.2.0 y anterior<br>• 8.3.0 y anterior | MySQL |
| OPatch, versión anterior a 12.2.0.1.42 | Global Lifecycle Management |
| OPatchAuto, versión anterior a 12.2.0.1.42 | Global Lifecycle Management |
| Oracle Access Manager, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Agile PLM, versión 9.3.6 | Oracle Supply Chain Componentes |
| Oracle Agile Componente Lifecycle Management for Process, versión 6.2.4.2 | Oracle Supply Chain Componentes |
| Oracle Application Testing Suite, versión 13.3.0.1 | Oracle Enterprise Manager |
| Oracle Banking APIs, versiones:<br>• 19.1.0.0.0<br>• 19.2.0.0.0<br>• 21.1.0.0.0 | Contact Support |

| | |
|---|---|
| • 22.1.0.0.0<br>• 22.2.0.0.0 | |
| Oracle Banking Branch, versiones:<br>• 14.5.0.0.0<br>• 14.6.0.0.0<br>• 14.7.0.0.0 | Contact Support |
| Oracle Banking Cash Management, versiones:<br>• 14.5.0.0.0<br>• 14.6.0.0.0<br>• 14.7.0.0.0 | Contact Support |
| Oracle Banking Deposits and Lines of Credit Servicing, versión 2.12.0.0.0 | Oracle Banking Deposits and Lines of Credit Servicing |
| Oracle Banking Digital Experience, versiones:<br>• 19.1.0.0.0<br>• 19.2.0.0.0<br>• 21.1.0.0.0<br>• 22.1.0.0.0<br>• 22.2.0.0.0 | Contact Support |
| Oracle Banking Enterprise Default Management, versiones:<br>• 2.7.0.0.0<br>• 2.12.0.0.0 | Oracle Banking Platform |
| Oracle Banking Liquidity Management, versiones:<br>• 14.5.0.0.0<br>• 14.6.0.0.0<br>• 14.7.0.0.0<br>• 14.7.0.3.0 | Contact Support |
| Oracle Banking Loans Servicing, versión 2.12.0.0.0 | Oracle Banking Platform |
| Oracle Banking Origination, versiones:<br>• 14.5.0.0.0<br>• 14.6.0.0.0<br>• 14.7.0.0.0 | Contact Support |
| Oracle Banking Party Management, versión 2.7.0.0.0 | Oracle Banking Platform |
| Oracle Banking Platform, versiones:<br>• 2.7.0.0.0<br>• 2.12.0.0.0 | Oracle Banking Platform |
| Oracle Banking Virtual Account Management, versiones:<br>• 14.5.0.0.0<br>• 14.6.0.0.0 | Contact Support |

| | |
|---|---|
| • 14.7.0.0.0 | |
| Oracle BI Publisher, versiones:<br>• 7.0.0.0.0<br>• 12.2.1.4.0 | Oracle Analytics |
| Oracle Big Data Spatial and Graph, versión 3.0.5 | Database |
| Oracle Business Intelligence Enterprise Edition, versiones:<br>• 7.0.0.0.0<br>• 12.2.1.4.0 | Oracle Analytics |
| Oracle Coherence, versiones:<br>• 12.2.1.4.0<br>• 14.1.1.0.0 | Fusion Middleware |
| Oracle Commerce Guided Search, versión 11.3.2 | Oracle Commerce |
| Oracle Commerce Platform, versiones:<br>• 11.3.0<br>• 11.3.1<br>• 11.3.2 | Oracle Commerce |
| Oracle Communications Billing and Revenue Management, versiones:<br>• 12.0.0.4 - 12.0.0.8<br>• 15.0.0.0 | Oracle Communications Billing and Revenue Management |
| Oracle Communications BRM - Elastic Charging Engine, versiones:<br>• 12.0.0.4 - 12.0.0.8<br>• 15.0.0.0 | Oracle Communications BRM - Elastic Charging Engine |
| Oracle Communications Cloud Native Core Binding Support Function, versiones 23.4.0 - 23.4.2 | Oracle Communications Cloud Native Core Binding Support Function |
| Oracle Communications Cloud Native Core Console, versión 23.4.0 | Oracle Communications Cloud Native Core Console |
| Oracle Communications Cloud Native Core Network Data Analytics Function, versión 24.1.0 | Oracle Communications Cloud Native Core Network Data Analytics Function |
| Oracle Communications Cloud Native Core Network Exposure Function, versión 23.4.1 | Oracle Communications Cloud Native Core Network Exposure Function |
| Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versiones:<br>• 23.2.0<br>• 23.3.1<br>• 23.4.0 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment |

| | |
|---|---|
| Oracle Communications Cloud Native Core Network Repository Function, versión 23.4.1 | Oracle Communications Cloud Native Core Network Repository Function |
| Oracle Communications Cloud Native Core Network Slice Selection Function, versiones:<br>• 23.2.0<br>• 23.3.0 | Oracle Communications Cloud Native Core Network Slice Selection Function |
| Oracle Communications Cloud Native Core Policy, versiones 23.4.0 - 23.4.2 | Oracle Communications Cloud Native Core Policy |
| Oracle Communications Cloud Native Core Security Edge Protection Proxy, versiones:<br>• 23.3.0<br>• 23.4.0 | Oracle Communications Cloud Native Core Security Edge Protection Proxy |
| Oracle Communications Cloud Native Core Service Communication Proxy, versiones:<br>• 23.1.0<br>• 23.2.2<br>• 23.3.0<br>• 23.4.0 | Oracle Communications Cloud Native Core Service Communication Proxy |
| Oracle Communications Cloud Native Core Unified Data Repository, versiones:<br>• 22.4.0<br>• 23.1.0<br>• 23.2.0<br>• 23.3.2 | Oracle Communications Cloud Native Core Unified Data Repository |
| Oracle Communications Diameter Signaling Router, versión 9.0.0.0 | Oracle Communications Diameter Signaling Router |
| Oracle Communications Element Manager, versiones 9.0.0 - 9.0.2 | Oracle Communications Element Manager |
| Oracle Communications Fraud Monitor, versiones:<br>• 5.0<br>• 5.1<br>• 5.2 | Oracle Communications Fraud Monitor |
| Oracle Communications Network Integrity, versión 7.3.6.4 | Oracle Communications Network Integrity |
| Oracle Communications Offline Mediation Controller, versiones 12.0.0.1 - 12.0.0.8 | Oracle Communications Offline Mediation Controller |
| Oracle Communications Operations Monitor, versiones:<br>• 5.0 | Oracle Communications Operations Monitor |

| | |
|---|---|
| • 5.1<br>• 5.2 | |
| Oracle Communications Service Catalog and Design, versión 8.0.0.1.0 | Oracle Communications Service Catalog and Design |
| Oracle Communications Session Report Manager, versiones 9.0.0 - 9.0.2 | Oracle Communications Session Report Manager |
| Oracle Communications Unified Inventory Management, versiones:<br>• 7.4.0 - 7.4.2<br>• 7.5.0<br>• 7.5.1 | Oracle Communications Unified Inventory Management |
| Oracle Communications User Data Repository, versión 14.0.0.0.0 | Oracle Communications User Data Repository |
| Oracle Communications WebRTC Session Controller, versiones 7.2.0.0.0 - 7.2.1.0.0 | Oracle Communications WebRTC Session Controller |
| Oracle Data Integrator, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Database Server, versiones:<br>• 19.3 - 19.22<br>• 21.3 - 21.13 | Database |
| Oracle Documaker, versión 12.6, 12.7 | Oracle Insurance Applications |
| Oracle E-Business Suite, versiones 12.2.3 - 12.2.13 | Oracle E-Business Suite |
| Oracle Enterprise Data Quality, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Enterprise Manager Base Platform, versión 13.5.0.0 | Oracle Enterprise Manager |
| Oracle Enterprise Manager for Fusion Middleware, versión 13.5.0.0 | Oracle Enterprise Manager |
| Oracle Essbase, versión 21.5.4.0.0 | Database |
| Oracle Financial Services Revenue Management and Billing, versiones:<br>• 2.8.0.0.0<br>• 2.9.0.0.0<br>• 2.9.0.1.0<br>• 3.0.0.0.0<br>• 3.1.0.0.0<br>• 3.2.0.0.0<br>• 4.0.0.0<br>• 5.0.0.0 | Oracle Financial Services Revenue Management and Billing |
| Oracle FLEXCUBE Private Banking, versión 12.1.0.0.0 | Contact Support |
| Oracle Fusion Middleware MapViewer, versión 12.2.1.4.0 | Fusion Middleware |

| | |
|---|---|
| Oracle Global Lifecycle Management NextGen OUI Framework, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle GoldenGate, versiones:<br>• 19.1.0.0.0 - 19.22.0.0.240124<br>• 21.3-21.13 | Database |
| Oracle GoldenGate Stream Analytics, versiones 19.1.0.0.0 - 19.1.0.0.8 | Database |
| Oracle GoldenGate Studio, versión 12.2.0.4.0 | Database |
| Oracle GoldenGate Veridata, versiones 12.2.1.4.0 - 12.2.1.4.230922 | Database |
| Oracle GraalVM Enterprise Edition, versiones:<br>• 20.3.13<br>• 21.3.9 | Java SE |
| Oracle GraalVM for JDK, versiones:<br>• 17.0.10<br>• 21.0.2<br>• 22 | Java SE |
| Oracle Healthcare Data Repository, versiones:<br>• 8.1.0.0<br>• 8.1.1.0<br>• 8.1.2.0<br>• 8.1.3.0<br>• 8.1.3.2<br>• 8.1.3.4 | HealthCare Applications |
| Oracle Hospitality Cruise Shipboard Property Management System, versiones:<br>• 20.3.3<br>• 20.3.4<br>• 23.1.0<br>• 23.1.1 | Oracle Hospitality Cruise Shipboard Property Management System |
| Oracle Hospitality Simphony, versiones 19.1.0 - 19.5.4 | Oracle Hospitality Simphony |
| Oracle HTTP Server, versiones:<br>• 12.2.1.4.0<br>• 14.1.1.0.0 | Fusion Middleware |
| Oracle Hyperion Infrastructure Technology, versión 11.2.16.0.0 | Oracle Enterprise Performance Management |
| Oracle Identity Manager, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Identity Manager Connector, versión 12.2.1.3.0 | Fusion Middleware |

| | |
|---|---|
| Oracle Internet Directory, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Java SE, versiones:<br>• 8u401<br>• 11.0.22<br>• 17.0.10<br>• 21.0.2<br>• 22 | Java SE |
| Oracle Life Sciences Empirica Signal, versiones:<br>• 9.1.0.53<br>• 9.2.0.53 | Health Sciences |
| Oracle Managed File Transfer, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Middleware Common Libraries and Tools, versiones:<br>• 12.2.1.4.0<br>• 14.1.1.0.0 | Fusion Middleware |
| Oracle Outside In Technology, versión 8.5.6, 8.5.7 | Fusion Middleware |
| Oracle Retail Assortment Planning, versiones:<br>• 15.0.3<br>• 16.0.3 | Retail Applications |
| Oracle Retail Customer Management and Segmentation Foundation, versión 19.0.0.9 | Retail Applications |
| Oracle Retail Integration Bus, versiones:<br>• 14.1.3.2<br>• 15.0.3.1<br>• 16.0.3<br>• 19.0.1 | Retail Applications |
| Oracle Retail Merchandising System, versiones:<br>• 14.1.3<br>• 15.0.3<br>• 16.0.3<br>• 19.0.1 | Retail Applications |
| Oracle Retail Sales Audit, versiones:<br>• 14.1.3.1<br>• 15.0.3.1<br>• 16.0.3<br>• 19.0.1 | Retail Applications |
| Oracle Retail Service Backbone, versiones: | Retail Applications |

| | |
|---|---|
| • 14.1.3.2<br>• 15.0.3.1<br>• 16.0.3<br>• 19.0.1 | |
| Oracle Retail Xstore Point of Service, versiones:<br>• 19.0.5<br>• 20.0.4<br>• 21.0.3<br>• 22.0.1<br>• 23.0.1 | Retail Applications |
| Oracle SD-WAN Edge, versión 9.1.1.7.0 | Oracle SD-WAN Edge |
| Oracle Smart View for Office, versión 11.2.16.0.0 | Oracle Enterprise Performance Management |
| Oracle SOA Suite, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle Solaris, versión 11 | Systems |
| Oracle Solaris Cluster, versión 4 | Systems |
| Oracle StorageTek Tape Analytics (STA), versión 2.5 | Systems |
| Oracle TimesTen In-Memory Database, versiones:<br>• anteriores a 22.1<br>• anteriores a 22.1.1.19.0<br>• anteriores a 22.1.1.23.0 | Database |
| Oracle Transportation Management, versiones:<br>• 6.5.2<br>• 6.5.3 | Oracle Supply Chain Componentes |
| Oracle Utilities Application Framework, versiones:<br>• 4.3.0.3.0 - 4.3.0.6.0<br>• 4.4.0.0.0<br>• 4.4.0.2.0<br>• 4.4.0.3.0<br>• 4.5.0.0.0<br>• 4.5.0.1.1<br>• 4.5.0.1.2 | Oracle Utilities Applications |
| Oracle Utilities Network Management System, versiones:<br>• 2.3.0.2<br>• 2.4.0.1<br>• 2.5.0.1<br>• 2.5.0.2<br>• 2.6.0.0<br>• 2.6.0.0.4 | Oracle Utilities Applications |

| | |
|---|---|
| • 2.6.0.1 | |
| Oracle VM VirtualBox, versione anteriores a 7.0.16 | Virtualization |
| Oracle Web Services Manager, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle WebCenter Content, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle WebCenter Enterprise Capture, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle WebCenter Portal, versión 12.2.1.4.0 | Fusion Middleware |
| Oracle WebLogic Server, versiones:<br>• 12.2.1.4.0<br>• 14.1.1.0.0 | Fusion Middleware |
| Oracle ZFS Storage Appliance Kit, versión 8.8 | Systems |
| OSS Support Tools, versiones:<br>• 2.12.44<br>• 2.12.45<br>• 23.1.23.1.17<br>• 24.1.24.1.16 | Oracle Support Tools |
| PeopleSoft Enterprise CRM Client Management, versión 9.2 | PeopleSoft |
| PeopleSoft Enterprise HCM Benefits Administration, versión 9.2 | PeopleSoft |
| PeopleSoft Enterprise PeopleTools, versiones:<br>• 8.59<br>• 8.60<br>• 8.61 | PeopleSoft |
| Primavera Gateway, versiones:<br>• 19.12.0 - 19.12.18<br>• 20.12.0 - 20.12.13<br>• 21.12.0 - 21.12.11 | Oracle Construction and Engineering Suite |
| Primavera P6 Enterprise Project Portfolio Management, versiones:<br>• 19.12.0 - 19.12.22<br>• 20.12.0 - 20.12.21<br>• 21.12.0 - 21.12.18<br>• 22.12.0 - 22.12.12<br>• 23.12.0 - 23.12.2 | Oracle Construction and Engineering Suite |
| Primavera Unifier, versiones:<br>• 19.12.0 - 19.12.16<br>• 20.12.0 - 20.12.16<br>• 21.12.0 - 21.12.17 | Oracle Construction and Engineering Suite |

| | |
|---|---|
| • 22.12.0 - 22.12.12<br>• 23.12.0 - 23.12.3 | |
| Siebel Applications, versión 24.2 y anteriores | Siebel |

## 3. Análisis técnico

A continuación, los detalles de las vulnerabilidades de más relevancia corregidas en esta actualización, que son los siguientes:

CVE-2024-1597: vulnerabilidad en el controlador JDBC de PostgreSQL, que permite a un atacante inyectar comandos SQL si utiliza *PreferQueryMode=SIMPLE*. Sin embargo, en el modo por defecto no hay vulnerabilidad.

La métrica de evaluación de esta vulnerabilidad se compone de:

CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection)

CVSS Base: **10.0**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario: Ninguna**
- **Alcance: Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21010, CVE-2024-20997: vulnerabilidades, **fácilmente explotables**, que permiten a un atacante con pocos privilegios y acceso a la red a través de HTTP poner en peligro Oracle Hospitality Simphony. Aunque las vulnerabilidades se encuentran en Oracle Hospitality Simphony, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de estas vulnerabilidades pueden resultar en la toma de control de Oracle Hospitality Simphon.

La métrica de evaluación de estas vulnerabilidades se compone de:

CVSS Base: **9.9**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario: Ninguna**
- **Alcance: Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21082: vulnerabilidad, **fácilmente explotable**, que permite a un atacante no autenticado con acceso a la red a través de HTTP poner en peligro Oracle BI Publisher. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle BI Publisher.

La métrica de evaluación de estas vulnerabilidades se compone de:

CVSS Base: **9.8**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario: Ninguna**
- **Alcance: Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21014: vulnerabilidad, **fácilmente explotable**, que permite a un atacante no autenticado con acceso a la red a través de HTTP poner en peligro Oracle Hospitality Simphony. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle Hospitality Simphony.

La métrica de evaluación de estas vulnerabilidades se compone de:

CVSS Base: **9.8**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario: Ninguna**
- **Alcance: Modificado**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21071: vulnerabilidad, **fácilmente explotable**, permite a un atacante con privilegios elevados con acceso a la red a través de HTTP poner en peligro Oracle Workflow. Aunque la vulnerabilidad se encuentra en Oracle Workflow, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle Workflow.

La métrica de evaluación de esta vulnerabilidad se compone de:

CVSS Base: **9.1**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario: Ninguna**
- **Alcance: Modificado**
- **Confidencialidad: Alta**
- **Integridad:Alta**
- **Disponibilidad: Alta**

CVE-2024-21115, CVE-2024-21114, CVE-2024-21113, CVE-2024-21112: vulnerabilidades, **fácilmente explotables**, que permiten a un atacante con pocos privilegios que inicie sesión en la infraestructura donde se ejecuta Oracle VM VirtualBox poner en peligro Oracle VM VirtualBox. Aunque las vulnerabilidades se encuentran en Oracle VM VirtualBox, los ataques pueden afectar significativamente a otros productos. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle VM VirtualBox.

CVE-2024-21067: vulnerabilidad, **fácilmente explotable**, permite a un atacante con pocos privilegios y con acceso a la infraestructura donde se ejecuta Oracle Enterprise Manager Base Platform comprometer Oracle Enterprise Manager Base Platform. Aunque la vulnerabilidad se encuentra en Oracle Enterprise Manager Base Platform, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle Enterprise Manager Base Platform.

La métrica de evaluación de estas vulnerabilidades se compone de:

CVSS Base: **8.8**

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque:** Local
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Bajo**
- **Interacción con el usuario: Ninguna**
- **Alcance: Modificado**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21626: *runc* es una herramienta CLI para crear y ejecutar contenedores en Linux de acuerdo con la especificación OCI. En *runc 1.1.11* y anteriores, debido a una fuga interna de descriptor de archivo, un atacante podría hacer que un proceso contenedor recién generado tuviera un directorio de trabajo en el espacio de nombres del sistema de archivos del host, permitiendo una fuga del contenedor dando acceso al sistema de archivos del host

La métrica de evaluación de esta vulnerabilidad se compone de:

CWE-668: Exposure of Resource to Wrong Sphere

CWE-403: Exposure of File Descriptor to Unintended Control Sphere (File Descriptor Leak)

CVSS Base: **8.6**

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

- **Vector de ataque:** Local
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario:** Requerida
- **Alcance: Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-20999: vulnerabilidad, **fácilmente explotable**, que permite a un atacante con altos privilegios iniciar sesión en la infraestructura donde se ejecuta Oracle Solaris poner en peligro Oracle Solaris. Aunque la vulnerabilidad está en Oracle Solaris, los ataques pueden afectar significativamente a productos adicionales. Los ataques exitosos de esta vulnerabilidad pueden resultar en la toma de control de Oracle Solaris.

La métrica de evaluación de esta vulnerabilidad se compone de:

CVSS Base: **8.2**

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque:** Local
- **Complejidad del ataque: Baja**
- **Privilegios requeridos:** Alta
- **Interacción con el usuario: Ninguna**
- **Alcance: Modificado**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2024-21095: vulnerabilidad, **fácilmente explotable**, que permite a un atacante no autenticado con acceso a la red a través de HTTP comprometer Primavera P6 Enterprise Project Portfolio Management. Los ataques exitosos de esta vulnerabilidad pueden resultar en acceso no autorizado a datos críticos o acceso completo a todos los datos accesibles de Primavera P6 Enterprise Project Portfolio Management, así como acceso no autorizado de actualización,

inserción o borrado a algunos de los datos accesibles de Primavera P6 Enterprise Project Portfolio Management.

CVE-2024-22257: Spring Security es vulnerable a un control de acceso cuando utiliza directamente el AuthenticatedVoter#vote pasando un parámetro de autenticación nulo.

La métrica de evaluación de estas vulnerabilidades se compone de:

CVSS Base: **8.2**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario: Ninguna**
- **Alcance:** Sin cambios
- **Confidencialidad: Alta**
- **Integridad:** Baja
- **Disponibilidad:** Ninguna

CVE-2024-22259: las aplicaciones que utilizan *UriComponentsBuilder* en Spring Framework para analizar una URL proporcionada y realizar comprobaciones de validación en el host de la URL analizada pueden ser vulnerables a un ataque de redirección abierta.

La métrica de evaluación de esta vulnerabilidad se compone de:

CVSS Base: **8.1**

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

- **Vector de ataque: Red**
- **Complejidad del ataque: Baja**
- **Privilegios requeridos: Ninguno**
- **Interacción con el usuario:** Requerida
- **Alcance: Sin cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad:** Ninguna

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

### Matriz de riesgos de Oracle Database Server

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-48795 | Grid Infrastructure (Apache Mina SSHD) | NaN | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle SQLcl (Apache Mina SSHD) | NaN | SSH | Sí | 5.9 |
| CVE-2024-21093 | Java VM | Create Session, Create Procedure | Oracle Net | No | 5.3 |
| CVE-2024-21058 | Unified Audit | SYSDBA | Oracle Net | No | 4.9 |
| CVE-2023-5072 | GraalVM Multilingual Engine | NaN | Multiple | Sí | 4.3 |
| CVE-2024-21066 | RDBMS | Authenticated User | NaN | No | 4.2 |
| CVE-2023-36632 | RDBMS (Python) | Authenticated User | Oracle Net | No | 3.5 |
| CVE-2024-20995 | Oracle Database Sharding | DBA | Oracle Net | No | 2.4 |

### Matriz de riesgos de Oracle Autonomous Health Framework

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-48795 | Autonomous Health Framework | CLI AND SDK (Paramiko) | SSH | Sí | 5.9 |

### Matriz de riesgo espacial y gráfica de Oracle Big Data

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-46589 | Oracle Big Data Spatial and Graph | Big Data Graph (Apache Tomcat) | HTTP | Sí | 7.5 |

### Matriz de riesgos de gestión del ciclo de vida global de Oracle

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-48795 | OPatchAuto | Database extensions (Apache Mina SSHD) | SSH | Sí | 5.9 |

### Matriz de riesgos de Oracle GoldenGate

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-5072 | Oracle GoldenGate Stream Analytics | Security (JSON-java) | HTTP | Sí | 7.5 |

### Matriz de riesgo de Oracle Commerce

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-46364 | Oracle Commerce Platform | Endeca Integration (Apache CXF) | HTTP | Sí | 9.8 |
| CVE-2023-1370 | Oracle Commerce Guided Search | Content Acquisition System, Workbench (json-smart) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-5072 | Oracle Commerce Platform | Platform (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2022-42003 | Oracle Commerce Platform | Platform (jackson-databind) | HTTP | Sí | 7.5 |
| CVE-2023-2976 | Oracle Commerce Guided Search | Content Acquisition System, Workbench (Google Guava) | NaN | No | 7.1 |
| CVE-2023-20863 | Oracle Commerce Platform | Platform (Spring Framework) | HTTP | No | 6.5 |
| CVE-2023-41080 | Oracle Commerce Guided Search | Workbench (Apache Tomcat) | HTTP | Sí | 6.1 |
| CVE-2024-21100 | Oracle Commerce Platform | Platform | HTTP | Sí | 4.0 |

Matrix Matriz de riesgos de las aplicaciones de Oracle Communications

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-47100 | Oracle Communications Billing and Revenue Management | Platform (Perl) | HTTP | Sí | 9.8 |
| CVE-2022-34381 | Oracle Communications Network Integrity | Platform (BSAFE Crypto-J) | HTTP | Sí | 9.8 |
| CVE-2022-34381 | Oracle Communications Unified Inventory Management | Security (BSAFE Crypto-J) | HTTPS | Sí | 9.8 |
| CVE-2023-44487 | Oracle Communications BRM - Elastic Charging Engine | Cloud Native Deployment (Netty) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-34053 | Oracle Communications BRM - Elastic Charging Engine | Security (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2024-21634 | Oracle Communications Service Catalog and Design | Patch (Amazon Ion) | HTTP | Sí | 7.5 |
| CVE-2023-4043 | Oracle Communications Service Catalog and Design | Patch (Eclipse Parsson) | HTTP | Sí | 7.5 |
| CVE-2023-6378 | Oracle Communications Service Catalog and Design | Patch (logback) | HTTP | Sí | 7.5 |
| CVE-2022-34169 | Oracle Communications Unified Inventory Management | General (Apache Xalan-Java) | HTTPS | Sí | 7.5 |
| CVE-2023-2976 | Oracle Communications Offline Mediation Controller | General (Google Guava) | NaN | No | 7.1 |
| CVE-2021-37533 | Oracle Communications Offline Mediation Controller | General (Apache Commons Net) | SFTP | Sí | 6.5 |
| CVE-2023-34055 | Oracle Communications Unified Inventory Management | General (Spring Boot) | HTTPS | No | 6.5 |
| CVE-2023-0833 | Oracle Communications Service Catalog and Design | Patch (OkHttp) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Communications Unified Inventory Management | General (Apache Commons Compress) | NaN | No | 5.5 |

## Matriz de riesgos de Oracle Communications

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-47100 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Perl) | HTTP | Sí | 9.8 |
| CVE-2023-43496 | Oracle Communications Cloud Native Core Network Slice Selection Function | Install/Upgrade (Jenkins) | HTTP | No | 8.8 |
| CVE-2023-4863 | Oracle Communications Diameter Signaling Router | Platform (libwebp) | HTTP | Sí | 8.8 |
| CVE-2024-21626 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Install/Upgrade (runc) | NaN | No | 8.6 |
| CVE-2024-21626 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Observability Services Overlay (runc) | NaN | No | 8.6 |
| CVE-2024-22257 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Spring Security) | HTTP | Sí | 8.2 |
| CVE-2024-22257 | Oracle Communications Cloud Native Core Console | Configuration (Spring Security) | HTTP | Sí | 8.2 |
| CVE-2024-22257 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Spring Security) | HTTP | Sí | 8.2 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-22259 | Oracle Communications Cloud Native Core Console | Configuration (Spring Web Services) | HTTP | Sí | 8.1 |
| CVE-2023-41056 | Oracle Communications Cloud Native Core Network Data Analytics Function | Third Party (Redis) | HTTP | Sí | 8.1 |
| CVE-2023-41056 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Redis) | HTTP | Sí | 8.1 |
| CVE-2023-41056 | Oracle Communications Operations Monitor | Infrastructure (Redis) | HTTP | Sí | 8.1 |
| CVE-2023-51257 | Oracle Communications Cloud Native Core Unified Data Repository | Install/Upgrade (JasPer) | NaN | No | 7.8 |
| CVE-2023-46589 | Management Cloud Engine | BEServer (Apache Tomcat) | HTTP | Sí | 7.5 |
| CVE-2023-34053 | Management Cloud Engine | BEServer (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2024-26130 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Cryptography) | HTTP | Sí | 7.5 |
| CVE-2024-22201 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Netty) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-44487 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Nghttp2) | HTTP | Sí | 7.5 |
| CVE-2022-40152 | Oracle Communications Cloud Native Core Console | Configuration (Keycloak) | HTTP | Sí | 7.5 |
| CVE-2023-46589 | Oracle Communications Cloud Native Core Network Data Analytics Function | Third Party (Apache Tomcat) | HTTP | Sí | 7.5 |
| CVE-2023-49083 | Oracle Communications Cloud Native Core Network Data Analytics Function | Third Party (Cryptography) | HTTP | Sí | 7.5 |
| CVE-2024-22233 | Oracle Communications Cloud Native Core Network Data Analytics Function | Third Party (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2024-22233 | Oracle Communications Cloud Native Core Network Exposure Function | Platform (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Installation (Nghttp2) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Observability Services Overlay (Golang Go) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-45142 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Observability Services Overlay (Prometheus) | HTTP | Sí | 7.5 |
| CVE-2024-25062 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Observability Services Overlay (libxml2) | HTTP | Sí | 7.5 |
| CVE-2023-5363 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Observability Services Overlay (nginx) | HTTP | Sí | 7.5 |
| CVE-2023-49083 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Cryptography) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Jenkins) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Nghttp2) | HTTP | Sí | 7.5 |
| CVE-2024-1635 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Undertow) | HTTP | Sí | 7.5 |
| CVE-2024-26130 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Cryptography) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-22201 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Netty) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Nghttp2) | HTTP | Sí | 7.5 |
| CVE-2023-49083 | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Automated Test Suite (Cryptography) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Automated Test Suite (Nghttp2) | HTTP | Sí | 7.5 |
| CVE-2024-22233 | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Signaling (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Automated Test Suite (Jenkins) | TCP | Sí | 7.5 |
| CVE-2022-45688 | Oracle Communications Cloud Native Core Service Communication Proxy | Install/Upgrade (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Cloud Native Core Service Communication Proxy | Install/Upgrade (Jenkins) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-49083 | Oracle Communications Cloud Native Core Unified Data Repository | Install/Upgrade (Cryptography) | HTTP | Sí | 7.5 |
| CVE-2024-22233 | Oracle Communications Cloud Native Core Unified Data Repository | Signaling (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2023-51775 | Oracle Communications Cloud Native Core Unified Data Repository | Signaling (jose4j) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Diameter Signaling Router | Patches (Nghttp2) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Communications Diameter Signaling Router | Platform (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-49083 | Oracle Communications Diameter Signaling Router | Automated Test Suite (Cryptography) | HTTPS | Sí | 7.5 |
| CVE-2023-31122 | Oracle Communications Element Manager | Security (Apache HTTP Server) | HTTP | Sí | 7.5 |
| CVE-2023-46589 | Oracle Communications Element Manager | Security (Apache Tomcat) | HTTP | Sí | 7.5 |
| CVE-2023-31122 | Oracle Communications Fraud Monitor | Mediation Engine (Apache HTTP Server) | HTTPS | Sí | 7.5 |
| CVE-2023-49083 | Oracle Communications Operations Monitor | Mediation Engine (Cryptography) | HTTPS | Sí | 7.5 |
| CVE-2023-31122 | Oracle Communications Session Report Manager | General (Apache HTTP Server) | HTTP | Sí | 7.5 |
| CVE-2023-46589 | Oracle Communications | General (Apache Tomcat) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| | Session Report Manager | | | | |
| CVE-2023-49083 | Oracle Communications User Data Repository | Security (Cryptography) | HTTPS | Sí | 7.5 |
| CVE-2023-5072 | Oracle Communications WebRTC Session Controller | Security (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2024-22233 | Oracle SD-WAN Edge | Internal tools (Spring Framework) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle SD-WAN Edge | User Interface (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-46589 | Oracle SD-WAN Edge | User Interface (Apache Tomcat) | HTTPS | Sí | 7.5 |
| CVE-2023-46589 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Apache Tomcat) | HTTP | Sí | 6.5 |
| CVE-2023-34055 | Oracle Communications Cloud Native Core Network Data Analytics Function | Third Party (Spring Boot) | HTTP | No | 6.5 |
| CVE-2023-2283 | Oracle Communications Cloud Native Core Network Slice Selection Function | Install/Upgrade (libssh) | SSH | Sí | 6.5 |
| CVE-2023-46589 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Apache Tomcat) | HTTP | Sí | 6.5 |
| CVE-2023-34055 | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Signaling (Spring Boot) | HTTP | No | 6.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-34055 | Oracle Communications Cloud Native Core Service Communication Proxy | Install/Upgrade (Spring Boot) | HTTP | No | 6.5 |
| CVE-2023-34055 | Oracle Communications Cloud Native Core Unified Data Repository | Install/Upgrade (Spring Boot) | HTTP | No | 6.5 |
| CVE-2023-34055 | Oracle SD-WAN Edge | User Interface (Spring Boot) | HTTP | No | 6.5 |
| CVE-2023-48795 | Oracle Communications Cloud Native Core Network Exposure Function | Install/Upgrade (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (libssh) | HTTP | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications Cloud Native Core Unified Data Repository | Install/Upgrade (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications Diameter Signaling Router | Patches (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications Element Manager | Security (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications Operations Monitor | Mediation Engine (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications Session Report Manager | General or Others (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Communications | Patches (Apache Mina SSHD) | SSH | Sí | 5.9 |

| | | | | | |
|---|---|---|---|---|---|
| | User Data Repository | | | | |
| CVE-2024-26308 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2023-4641 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (shadow-utils) | NaN | No | 5.5 |
| CVE-2022-40896 | Oracle Communications Cloud Native Core Network Repository Function | Install/Upgrade (Pygments) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2023-4641 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (shadow-utils) | NaN | No | 5.5 |
| CVE-2022-40896 | Oracle Communications Cloud Native Core Security Edge Protection Proxy | Installation and Configuration (Pygments) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Communications Cloud Native Core Unified Data Repository | Install/Upgrade (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Communications Element Manager | Security (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2023-5341 | Oracle Communications Operations Monitor | Infrastructure (ImageMagick) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Communications | General or Others (Apache | NaN | No | 5.5 |

| | | | | | |
|---|---|---|---|---|---|
| | Session Report Manager | Commons Compress) | | | |
| CVE-2023-51074 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (JsonPath) | HTTP | Sí | 5.3 |
| CVE-2023-33201 | Oracle Communications Cloud Native Core Network Function Cloud Native Environment | Configuration (Bouncy Castle Java Library) | HTTPS | Sí | 5.3 |
| CVE-2023-51074 | Oracle Communications Cloud Native Core Policy | Install/Upgrade (JsonPath) | HTTP | Sí | 5.3 |
| CVE-2023-33201 | Oracle Communications Cloud Native Core Service Communication Proxy | Install/Upgrade (Bouncy Castle Java Library) | HTTPS | Sí | 5.3 |
| CVE-2023-6507 | Oracle Communications Cloud Native Core Network Data Analytics Function | Third Party (Python) | HTTP | No | 4.9 |
| CVE-2023-4016 | Oracle Communications Cloud Native Core Binding Support Function | Install/Upgrade (procps) | NaN | No | 3.3 |
| CVE-2023-4016 | Oracle Communications Cloud Native Core Policy | Policy (procps) | NaN | No | 3.3 |

## Matrix Matriz de riesgos de construcción e ingeniería de Oracle

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-21095 | Primavera P6 Enterprise | Web Access | HTTP | Sí | 8.2 |

| | | | | | |
|---|---|---|---|---|---|
| | Project Portfolio Management | | | | |
| CVE-2023-5072 | Primavera Gateway | Admin (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-52428 | Primavera Unifier | Integration (Nimbus JOSE+JWT) | HTTP | Sí | 7.5 |
| CVE-2023-50386 | Primavera Unifier | Document Management (Apache Solr) | HTTP | No | 6.3 |
| CVE-2024-26308 | Primavera Gateway | Admin (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Primavera Unifier | Platform (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-22243 | Primavera Unifier | Document Management (Spring Framework) | HTTP | Sí | 5.4 |

## Matriz de riesgos de Oracle E-Business Suite

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-21071 | Oracle Workflow | Admin Screens and Grants UI | HTTP | No | 9.1 |
| CVE-2024-21078 | Oracle Marketing | Campaign LOV | HTTP | Sí | 7.5 |
| CVE-2024-21079 | Oracle Marketing | Campaign LOV | HTTP | Sí | 7.5 |
| CVE-2024-21088 | Oracle Componenteion Scheduling | Import Utility | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21073 | Oracle Trade Management | Claim LOV | HTTP | Sí | 7.5 |
| CVE-2024-21075 | Oracle Trade Management | Claim Line LOV | HTTP | Sí | 7.5 |
| CVE-2024-21074 | Oracle Trade Management | Finance LOV | HTTP | Sí | 7.5 |
| CVE-2024-21077 | Oracle Trade Management | GL Accounts LOV | HTTP | Sí | 7.5 |
| CVE-2024-21076 | Oracle Trade Management | Offer LOV | HTTP | Sí | 7.5 |
| CVE-2024-21080 | Oracle Applications Framework | REST Services | HTTP | No | 6.5 |
| CVE-2024-21089 | Oracle Concurrent Processing | Request Submission and Scheduling | HTTP | No | 6.5 |
| CVE-2024-21016 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21017 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21018 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21019 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21020 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21021 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21022 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21023 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21024 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21025 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21026 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21027 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21028 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21029 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21030 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21031 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21032 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21033 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21034 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21035 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21036 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21037 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21038 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21039 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21040 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21041 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21042 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21043 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21044 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21045 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21046 | Oracle Complex Maintenance, Repair, and Overhaul | LOV | HTTP | Sí | 6.1 |
| CVE-2024-21072 | Oracle Installed Base | Data Provider UI | HTTP | Sí | 6.1 |
| CVE-2024-20990 | Oracle Applications Technology | Templates | HTTP | Sí | 5.3 |
| CVE-2024-21081 | Oracle Partner Management | Attribute Admin Setup | HTTP | Sí | 4.7 |
| CVE-2024-21086 | Oracle CRM Technical Foundation | Preferences | HTTP | Sí | 4.3 |
| CVE-2024-21048 | Oracle Web Applications Desktop Integrator | XML input | HTTP | No | 4.3 |

## Matriz de riesgos de Oracle Enterprise Manager

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-42920 | Oracle Application Testing Suite | Load Testing for Web Apps (Apache Commons BCEL) | HTTP | Sí | 9.8 |
| CVE-2022-46337 | Oracle Application Testing Suite | Load Testing for Web Apps (Apache Derby) | HTTP | Sí | 9.8 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-34381 | Oracle Application Testing Suite | Load Testing for Web Apps (BSAFE Crypto-J) | HTTP | Sí | 9.8 |
| CVE-2022-42920 | Oracle Enterprise Manager for Fusion Middleware | Enterprise Manager Install (Apache Commons BCEL) | HTTP | Sí | 9.8 |
| CVE-2024-21067 | Oracle Enterprise Manager Base Platform | Host Management | NaN | No | 8.8 |
| CVE-2021-36770 | Oracle Enterprise Manager for Fusion Middleware | Provisioning (Perl) | NaN | No | 7.8 |
| CVE-2023-1370 | Oracle Application Testing Suite | Load Testing for Web Apps (json-smart) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Enterprise Manager Base Platform | Job System (Netty) | HTTP | Sí | 7.5 |
| CVE-2023-20861 | Oracle Enterprise Manager for Fusion Middleware | Install (Spring Framework) | HTTP | No | 6.5 |
| CVE-2023-48795 | Oracle Enterprise Manager Base Platform | Enterprise Manager Install (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-42503 | Oracle Enterprise Manager Base Platform | Enterprise Manager Install (Apache Commons Compress) | NaN | No | 5.5 |

Matrix Matriz de riesgos de las aplicaciones de Oracle Financial Services

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-46604 | Oracle FLEXCUBE Private Banking | Miscellaneous (Apache ActiveMQ) | HTTP | No | 8.8 |
| CVE-2022-46337 | Oracle FLEXCUBE Private Banking | Miscellaneous (Apache Derby) | HTTP | No | 8.8 |
| CVE-2023-44981 | Oracle Banking Branch | Reports (Apache ZooKeeper) | HTTP | No | 8.1 |
| CVE-2023-44981 | Oracle Banking Cash Management | Accessibility (Apache ZooKeeper) | HTTP | No | 8.1 |
| CVE-2023-44981 | Oracle Banking Liquidity Management | Common (Apache ZooKeeper) | HTTP | No | 8.1 |
| CVE-2023-44981 | Oracle Banking Origination | Basic Config/Maintenances (Apache ZooKeeper) | HTTP | No | 8.1 |
| CVE-2023-44981 | Oracle Banking Virtual Account Management | Common Core (Apache ZooKeeper) | HTTP | No | 8.1 |
| CVE-2023-44487 | Oracle Banking Branch | Reports (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Branch | Reports (Netty) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-44487 | Oracle Banking Cash Management | Accessibility (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Cash Management | Accessibility (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Cash Management | Accessibility (Netty) | HTTP | Sí | 7.5 |
| CVE-2023-2618 | Oracle Banking Cash Management | Accessibility (OpenCV) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Deposits and Lines of Credit Servicing | Web UI (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Enterprise Default Management | Collections (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Liquidity Management | Common (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Liquidity Management | Common (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Liquidity | Common (Netty) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| | Management | | | | |
| CVE-2023-44271 | Oracle Banking Liquidity Management | Common (Pillow) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Liquidity Management | Infrastructure (gRPC) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Loans Servicing | Web UI (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-46589 | Oracle Banking Origination | Basic Config/Maintenances (Apache Tomcat) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Origination | Basic Config/Maintenances (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Origination | Basic Config/Maintenances (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Origination | Basic Config/Maintenances (Netty) | HTTP | Sí | 7.5 |
| CVE-2023-44271 | Oracle Banking Origination | Basic Config/Maintenances (Pillow) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Party Management | Web UI (Netty) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Platform | Security (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023- | Oracle Banking Platform | Security (Netty) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| 44487 | | | | | |
| CVE-2023-44487 | Oracle Banking Virtual Account Management | Common Core (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle Banking Virtual Account Management | Common Core (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle Banking Virtual Account Management | Common Core (Netty) | HTTP | Sí | 7.5 |
| CVE-2023-2618 | Oracle Banking Virtual Account Management | Common Core (OpenCV) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle FLEXCUBE Private Banking | Miscellaneous (Eclipse Jetty) | HTTP | Sí | 7.5 |
| CVE-2023-44483 | Oracle Banking Branch | Reports (Apache Santuario XML Security For Java) | HTTP | No | 6.5 |
| CVE-2023-44483 | Oracle Banking Cash Management | Accessibility (Apache Santuario XML Security For Java) | HTTP | No | 6.5 |
| CVE-2023-44483 | Oracle Banking Liquidity Management | Common (Apache Santuario XML Security For Java) | HTTP | No | 6.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-44483 | Oracle Banking Origination | Basic Config/Maintenances (Apache Santuario XML Security For Java) | HTTP | No | 6.5 |
| CVE-2023-44483 | Oracle Banking Virtual Account Management | Common Core (Apache Santuario XML Security For Java) | HTTP | No | 6.5 |
| CVE-2024-23635 | Oracle Banking Party Management | Web UI (AntiSamy) | HTTP | Sí | 6.1 |
| CVE-2022-31160 | Oracle Financial Services Revenue Management and Billing | Infrastructure (jQueryUI) | HTTP | Sí | 6.1 |
| CVE-2024-26308 | Oracle Banking APIs | IDM - Authentication (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Banking Deposits and Lines of Credit Servicing | Web UI (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Banking Digital Experience | UI General (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Banking Loans Servicing | Web UI (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2023-42503 | Oracle Banking Party Management | Web UI (Apache Commons Compress) | NaN | No | 5.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-26308 | Oracle Banking Platform | Security (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle Financial Services Revenue Management and Billing | IP - Installation Upgrade Proc (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2023-33201 | Oracle Banking Party Management | Web UI (Bouncy Castle Java Library) | LDAP | Sí | 5.3 |

## Matriz de riesgos de aplicaciones de alimentos y bebidas de Oracle

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-20997 | Oracle Hospitality Simphony | Simphony Enterprise Server | HTTP | No | 9.9 |
| CVE-2024-21010 | Oracle Hospitality Simphony | Simphony Enterprise Server | HTTP | No | 9.9 |
| CVE-2024-21014 | Oracle Hospitality Simphony | Simphony Enterprise Server | HTTP | Sí | 9.8 |
| CVE-2024-20989 | Oracle Hospitality Simphony | Simphony POS | HTTP | Sí | 7.0 |

## Matriz de riesgos de Oracle Fusion Middleware

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-46337 | Oracle Enterprise Data Quality | Third Party (Apache Derby) | HTTP | Sí | 9.8 |
| CVE-2024-1597 | Oracle Enterprise Data Quality | Third Party (PostgreSQL JDBC Driver) | HTTP | Sí | 9.8 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-46337 | Oracle Fusion Middleware MapViewer | Map Builder (Apache Derby) | HTTP | Sí | 9.8 |
| CVE-2022-34381 | Oracle HTTP Server | Plugins (BSAFE Crypto-J) | TLS | Sí | 9.8 |
| CVE-2019-13990 | Oracle Identity Manager | Third Party (Quartz) | HTTP | Sí | 9.8 |
| CVE-2019-13990 | Oracle Internet Directory | Directory Integration Platform (Quartz) | HTTP | Sí | 9.8 |
| CVE-2022-46337 | Oracle Middleware Common Libraries and Tools | Third Party (Apache Derby) | HTTP | Sí | 9.8 |
| CVE-2022-1471 | Oracle SOA Suite | Third Party (SnakeYAML) | HTTP | Sí | 9.8 |
| CVE-2022-45378 | Oracle Web Services Manager | Third Party (Apache SOAP) | HTTP | Sí | 9.8 |
| CVE-2021-23369 | Oracle WebLogic Server | Samples (handlebars) | HTTP | Sí | 9.8 |
| CVE-2023-37536 | Oracle Access Manager | Webserver Plugin (Apache Xerces-C++) | HTTP | No | 8.8 |
| CVE-2023-37536 | Oracle SOA Suite | Third Party (Apache Xerces-C++) | HTTP | No | 8.8 |
| CVE-2019-0231 | Oracle Access Manager | Third Party (Apache Mina) | TLS | Sí | 7.5 |
| CVE-2023-44487 | Oracle Data Integrator | Runtime Java agent for ODI (Eclipse Jetty) | HTTP/2 | Sí | 7.5 |
| CVE-2023-31122 | Oracle HTTP Server | Third Party (Apache HTTP Server) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-24021 | Oracle HTTP Server | SSL Module (ModSecurity) | TLS | Sí | 7.5 |
| CVE-2023-5072 | Oracle Identity Manager Connector | Third Party (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2022-42003 | Oracle Identity Manager Connector | Third Party (jackson-databind) | HTTP | Sí | 7.5 |
| CVE-2023-46589 | Oracle Managed File Transfer | MFT Runtime Server (Apache Tomcat) | HTTP | Sí | 7.5 |
| CVE-2019-10172 | Oracle WebCenter Content | ADF UCM Application (jackson-mapper-asl) | HTTP | Sí | 7.5 |
| CVE-2023-3635 | Oracle WebCenter Enterprise Capture | Third Party (Okio) | HTTP | Sí | 7.5 |
| CVE-2023-5072 | Oracle WebLogic Server | Centralized Thirdparty Jars (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-52428 | Oracle WebLogic Server | Core (Nimbus JOSE+JWT) | HTTP | Sí | 7.5 |
| CVE-2023-44487 | Oracle WebLogic Server | Web Container | HTTP/2 | Sí | 7.5 |
| CVE-2024-21006 | Oracle WebLogic Server | Core | T3, IIOP | Sí | 7.5 |
| CVE-2024-21007 | Oracle WebLogic Server | Core | T3, IIOP | Sí | 7.5 |
| CVE-2023-2976 | Oracle Data Integrator | Data Transforms (Jython) | NaN | No | 7.1 |
| CVE-2023-2976 | Oracle Identity Manager Connector | Google Cloud Connector (Google Guava) | NaN | No | 7.1 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-2976 | Oracle WebLogic Server | WLST (Python) | NaN | No | 7.1 |
| CVE-2022-25147 | Oracle HTTP Server | SSL Module (Apache Portable Runtime Utility) | TLS | Sí | 6.5 |
| CVE-2023-46218 | Oracle HTTP Server | SSL Module (curl) | TLS | Sí | 6.5 |
| CVE-2022-34169 | Oracle Outside In Technology | Outside In Clean Content SDK (Apache Xalan-Java) | NaN | No | 6.2 |
| CVE-2022-48579 | Oracle Outside In Technology | Outside In Core (unrar) | NaN | No | 6.2 |
| CVE-2024-23635 | Oracle WebLogic Server | Centralized Thirdparty Jars (AntiSamy) | HTTP | Sí | 6.1 |
| CVE-2023-48795 | Oracle Coherence | Third Party (Apache Mina SSHD) | SFTP | Sí | 5.9 |
| CVE-2023-48795 | Oracle Global Lifecycle Management NextGen OUI Framework | NextGen Installer (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle Middleware Common Libraries and Tools | Remote Diagnostic Agent (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | Oracle SOA Suite | Adapters (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2024-26308 | Oracle Enterprise Data Quality | Third Party (Apache Commons Compress) | NaN | No | 5.5 |
| CVE-2024-26308 | Oracle WebLogic Server | Centralized Thirdparty Jars (Apache | NaN | No | 5.5 |

| | | | | | |
|---|---|---|---|---|---|
| | | Commons Compress) | | | |
| CVE-2022-24329 | Oracle Access Manager | Third Party (JetBrains Kotlin) | HTTP | Sí | 5.3 |
| CVE-2024-20991 | Oracle HTTP Server | Web Listener | HTTP | Sí | 5.3 |
| CVE-2024-21119 | Oracle Outside In Technology | Outside In Core | NaN | No | 5.3 |
| CVE-2024-21117 | Oracle Outside In Technology | Outside In Core | NaN | No | 5.3 |
| CVE-2024-21120 | Oracle Outside In Technology | Outside In Core | NaN | No | 5.3 |
| CVE-2024-21118 | Oracle Outside In Technology | Outside In Core | NaN | No | 5.3 |
| CVE-2023-33201 | Oracle SOA Suite | Third Party (Bouncy Castle Java Library) | TLS | Sí | 5.3 |
| CVE-2023-33201 | Oracle WebLogic Server | Centralized Thirdparty Jars (Bouncy Castle Java Library) | Multiple | Sí | 5.3 |
| CVE-2023-35116 | Oracle Identity Manager | Third Party (jackson-databind) | NaN | No | 4.7 |
| CVE-2024-20992 | Oracle WebCenter Portal | Content integration | HTTP | No | 4.4 |
| CVE-2023-35887 | Oracle Data Integrator | Users, roles, credentials, security (Apache Mina) | SSH | No | 4.3 |

Matriz de riesgos de Oracle Analytics

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-21082 | Oracle BI Publisher | XML Services | HTTP | Sí | 9.8 |
| CVE-2023-43804 | Oracle Business Intelligence Enterprise Edition | Analytics Server (urllib3) | HTTP | No | 8.1 |
| CVE-2022-42890 | Oracle Business Intelligence Enterprise Edition | Analytics Web General (Apache Batik) | HTTP | Sí | 7.5 |
| CVE-2021-28861 | Oracle Business Intelligence Enterprise Edition | Data Visualization (Python) | HTTP | Sí | 7.4 |
| CVE-2024-21083 | Oracle BI Publisher | Script Engine | HTTP | No | 7.2 |
| CVE-2023-2976 | Oracle Business Intelligence Enterprise Edition | Data Visualization, Installation (Google Guava) | NaN | No | 7.1 |
| CVE-2024-21084 | Oracle BI Publisher | Service Gateway | HTTP | Sí | 5.8 |
| CVE-2024-21064 | Oracle Business Intelligence Enterprise Edition | Analytics Web Answers | HTTP | No | 5.4 |
| CVE-2024-21001 | Oracle Business Intelligence Enterprise Edition | BI Platform Security | HTTP | No | 5.4 |
| CVE-2023-3817 | Oracle Business Intelligence | Installation (OpenSSL) | TLS | Sí | 5.3 |

| | | | | | |
|---|---|---|---|---|---|
| | Enterprise Edition | | | | |
| CVE-2023-35116 | Oracle Business Intelligence Enterprise Edition | Analytics Server (jackson-databind) | NaN | No | 4.7 |
| CVE-2024-21099 | Oracle Business Intelligence Enterprise Edition | Data Visualization | HTTP | No | 4.3 |

### Matriz de riesgos de las aplicaciones de Oracle Health Sciences

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-5072 | Oracle Life Sciences Empirica Signal | Core (JSON-java) | HTTP | No | 6.5 |
| CVE-2023-42503 | Oracle Life Sciences Empirica Signal | Core (Apache Commons Compress) | NaN | No | 5.0 |

### Matriz de riesgos de las aplicaciones de Oracle HealthCare

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-42889 | Oracle Healthcare Data Repository | FHIR (Apache Commons Text) | HTTP | Sí | 9.8 |
| CVE-2023-2976 | Oracle Healthcare Data Repository | FHIR (Google Guava) | NaN | No | 7.1 |
| CVE-2023-20863 | Oracle Healthcare Data Repository | FHIR (Spring Framework) | HTTP | No | 6.5 |

### Matriz de riesgos de Oracle Hospitality Applications

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-6378 | Oracle Hospitality Cruise Shipboard Property Management System | APIs (Helidon) | HTTP | Sí | 7.5 |

### Matriz de riesgos de Oracle Hyperion

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-6246 | Oracle Hyperion Infrastructure Technology | Installation and Configuration (glibc) | NaN | No | 7.8 |
| CVE-2023-29081 | Oracle Smart View for Office | Authentication (InstallShield) | NaN | No | 5.5 |

### Matriz de riesgos de Oracle Insurance Applications

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-46337 | Oracle Documaker | Development Tools (Apache Derby) | HTTP | Sí | 9.8 |
| CVE-2021-43113 | Oracle Documaker | Enterprise Edition (iTextPDF) | NaN | No | 7.8 |
| CVE-2021-41616 | Oracle Documaker | Enterprise Edition (Apache DB DdlUtils) | SQL | No | 7.2 |
| CVE-2022-41853 | Oracle Documaker | Enterprise Edition (HyperSQL Database) | NaN | No | 6.7 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-24816 | Oracle Documaker | Enterprise Edition (CKEditor) | HTTP | Sí | 6.1 |
| CVE-2023-37536 | Oracle Documaker | Development Tools (Apache Xerces-C++) | NaN | No | 2.9 |

## Matriz de riesgos de Oracle Java SE

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-21892 | Oracle GraalVM for JDK | Node (Node.js) | NaN | No | 7.5 |
| CVE-2023-41993 | Oracle Java SE, Oracle GraalVM Enterprise Edition | JavaFX (WebKitGTK) | Multiple | Sí | 7.5 |
| CVE-2024-20954 | Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition | Compiler | Multiple | Sí | 3.7 |
| CVE-2024-21098 | Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition | Compiler | Multiple | Sí | 3.7 |
| CVE-2024-21085 | Oracle Java SE, Oracle GraalVM Enterprise Edition | Concurrency | Multiple | Sí | 3.7 |
| CVE-2024-21011 | Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition | Hotspot | Multiple | Sí | 3.7 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21068 | Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition | Hotspot | Multiple | Sí | 3.7 |
| CVE-2024-21094 | Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition | Hotspot | Multiple | Sí | 3.7 |
| CVE-2024-21012 | Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition | Networking | Multiple | Sí | 3.7 |
| CVE-2024-21003 | Oracle Java SE, Oracle GraalVM Enterprise Edition | JavaFX | Multiple | Sí | 3.1 |
| CVE-2024-21005 | Oracle Java SE, Oracle GraalVM Enterprise Edition | JavaFX | Multiple | Sí | 3.1 |
| CVE-2024-21002 | Oracle Java SE, Oracle GraalVM Enterprise Edition | JavaFX | NaN | No | 2.5 |
| CVE-2024-21004 | Oracle Java SE, Oracle GraalVM Enterprise Edition | JavaFX | NaN | No | 2.5 |

Matriz de riesgos de Oracle MySQL

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-44487 | MySQL Cluster | Cluster: General (Nghttp2) | Multiple | Sí | 7.5 |
| CVE-2024-21090 | MySQL Connectors | Connector/Python | X Protocolo | Sí | 7.5 |
| CVE-2023-6129 | MySQL Connectors | Connector/C++ (OpenSSL) | MySQL Protocolo | Sí | 6.5 |
| CVE-2023-6129 | MySQL Connectors | Connector/ODBC (OpenSSL) | MySQL Protocolo | Sí | 6.5 |
| CVE-2023-6129 | MySQL Enterprise Backup | Enterprise Backup (OpenSSL) | TLS | Sí | 6.5 |
| CVE-2023-6129 | MySQL Enterprise Monitor | Monitoring: General (OpenSSL) | Multiple | Sí | 6.5 |
| CVE-2023-6129 | MySQL Server | Server: Packaging (OpenSSL) | TLS | Sí | 6.5 |
| CVE-2024-21015 | MySQL Server | Server: DML | MySQL Protocolo | No | 5.5 |
| CVE-2024-0853 | MySQL Cluster | Cluster: General (curl) | Multiple | Sí | 5.3 |
| CVE-2024-0853 | MySQL Enterprise Backup | Enterprise Backup (curl) | HTTP | Sí | 5.3 |
| CVE-2024-20994 | MySQL Server | Server: Information Schema | MySQL Protocolo | No | 5.3 |
| CVE-2024-21102 | MySQL Cluster | Cluster: General | Multiple | No | 4.9 |
| CVE-2024-21047 | MySQL Server | InnoDB | MySQL Protocolo | No | 4.9 |
| CVE-2024-21061 | MySQL Server | Server: Audit Plug-in | MySQL Protocolo | No | 4.9 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21069 | MySQL Server | Server: DDL | MySQL Protocolo | No | 4.9 |
| CVE-2024-21049 | MySQL Server | Server: DML | MySQL Protocolo | No | 4.9 |
| CVE-2024-21050 | MySQL Server | Server: DML | MySQL Protocolo | No | 4.9 |
| CVE-2024-21051 | MySQL Server | Server: DML | MySQL Protocolo | No | 4.9 |
| CVE-2024-21052 | MySQL Server | Server: DML | MySQL Protocolo | No | 4.9 |
| CVE-2024-21053 | MySQL Server | Server: DML | MySQL Protocolo | No | 4.9 |
| CVE-2024-21056 | MySQL Server | Server: DML | MySQL Protocolo | No | 4.9 |
| CVE-2024-21060 | MySQL Server | Server: Data Dictionary | MySQL Protocolo | No | 4.9 |
| CVE-2024-21087 | MySQL Server | Server: Group Replication Plugin | MySQL Protocolo | No | 4.9 |
| CVE-2024-20993 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |
| CVE-2024-20998 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |
| CVE-2024-21009 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |
| CVE-2024-21054 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |
| CVE-2024-21055 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |
| CVE-2024-21057 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21062 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.9 |
| CVE-2024-21102 | MySQL Server | Server: Thread Pooling | MySQL Protocolo | No | 4.9 |
| CVE-2024-21096 | MySQL Server | Client: mysqldump | NaN | No | 4.9 |
| CVE-2024-21008 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.4 |
| CVE-2024-21013 | MySQL Server | Server: Optimizer | MySQL Protocolo | No | 4.4 |
| CVE-2024-21000 | MySQL Server | Server: Security: Privileges | MySQL Protocolo | No | 3.8 |
| CVE-2024-21101 | MySQL Cluster | Cluster: General | Multiple | No | 2.2 |

## Matriz de riesgos de Oracle PeopleSoft

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-38545 | PeopleSoft Enterprise PeopleTools | File Processing (curl) | HTTP | Sí | 9.8 |
| CVE-2023-4807 | PeopleSoft Enterprise PeopleTools | Security (OpenSSL) | NaN | No | 7.8 |
| CVE-2023-4043 | PeopleSoft Enterprise PeopleTools | Security (Eclipse Parsson) | HTTP | Sí | 7.5 |
| CVE-2021-37533 | PeopleSoft Enterprise CRM Client Management | Third Party (Apache Commons Net) | HTTP | Sí | 6.5 |
| CVE-2023-44483 | PeopleSoft Enterprise CRM Client Management | Third Party (Apache Santuario XML Security For Java) | HTTP | No | 6.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21063 | PeopleSoft Enterprise HCM Benefits Administration | Benefits Administration | NaN | No | 6.1 |
| CVE-2024-21065 | PeopleSoft Enterprise PeopleTools | Workflow | HTTP | Sí | 6.1 |
| CVE-2022-24613 | PeopleSoft Enterprise PeopleTools | OpenSearch (metadata-extractor) | NaN | No | 5.5 |
| CVE-2024-21070 | PeopleSoft Enterprise PeopleTools | Search Framework | HTTP | Sí | 5.4 |
| CVE-2024-21097 | PeopleSoft Enterprise PeopleTools | Security | HTTP | No | 4.9 |

## Matriz de riesgos de Oracle Retail Applications

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-42920 | Oracle Retail Assortment Planning | Application Core (Apache Commons BCEL) | HTTP | Sí | 9.8 |
| CVE-2022-46337 | Oracle Retail Integration Bus | RIB Kernal (Apache Derby) | HTTP | Sí | 9.8 |
| CVE-2022-34381 | Oracle Retail Integration Bus | RIB Kernal (BSAFE Crypto-J) | HTTP | Sí | 9.8 |
| CVE-2022-34381 | Oracle Retail Service Backbone | Install (BSAFE Crypto-J) | HTTP | Sí | 9.8 |
| CVE-2023-1436 | Oracle Retail Merchandising System | Security (Jettison) | HTTP | Sí | 7.5 |
| CVE-2023-1436 | Oracle Retail Sales Audit | Other (Jettison) | HTTP | Sí | 7.5 |
| CVE-2023-34981 | Oracle Retail Xstore Point of Service | Xenvironment (Apache Tomcat) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-2976 | Oracle Retail Xstore Point of Service | Xenvironment (Google Guava) | NaN | No | 7.1 |
| CVE-2022-31160 | Oracle Retail Customer Management and Segmentation Foundation | Internal Operations (jQueryUI) | HTTP | Sí | 6.1 |
| CVE-2023-48795 | Oracle Retail Customer Management and Segmentation Foundation | Internal Operations (Apache Mina SSHD) | SSH | Sí | 5.9 |

## Matriz de riesgos de Oracle Siebel CRM

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-2976 | Siebel Apps - Public Sector | Other (Google Guava) | NaN | No | 7.1 |

## Matriz de riesgos de Oracle Supply Chain

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-21092 | Oracle Agile Componente Lifecycle Management for Process | Componente Quality Management | HTTP | No | 8.1 |
| CVE-2023-46589 | Oracle Agile PLM | Security (Apache Tomcat) | HTTP | Sí | 7.5 |
| CVE-2023-24998 | Oracle Transportation Management | Install (Apache Commons FileUpload) | HTTP | Sí | 7.5 |
| CVE-2022-34169 | Oracle Transportation Management | Install (Apache Xalan-Java) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21091 | Oracle Agile Componente Lifecycle Management for Process | Data Import | HTTP | No | 6.5 |
| CVE-2023-42503 | Oracle Transportation Management | Install (Apache Tika) | NaN | No | 5.5 |

## Matriz de riesgos de Oracle Support Tools

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2023-1370 | OSS Support Tools | DA - Diagnostic Assistant (json-smart) | HTTP | Sí | 7.5 |
| CVE-2023-1370 | OSS Support Tools | RDA - Remote Diagnostic Agent (json-smart) | HTTP | Sí | 7.5 |
| CVE-2023-1370 | OSS Support Tools | STB - Services Tools Bundle (json-smart) | HTTP | Sí | 7.5 |
| CVE-2023-48795 | OSS Support Tools | DA - Diagnostic Assistant (Apache Mina SSHD) | SSH | Sí | 5.9 |
| CVE-2023-48795 | OSS Support Tools | RDA - Remote Diagnostic Agent (Apache Mina SSHD) | SSH | Sí | 5.9 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2023-48795 | OSS Support Tools | STB - Services Tools Bundle (Apache Mina SSHD) | SSH | Sí | 5.9 |

## Matriz de riesgos de Oracle Systems

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2022-42920 | Oracle Solaris Cluster | Tools (Apache Commons BCEL) | HTTP | Sí | 9.8 |
| CVE-2022-42920 | Oracle StorageTek Tape Analytics (STA) | Core (Apache Commons BCEL) | HTTP | Sí | 9.8 |
| CVE-2022-34381 | Oracle StorageTek Tape Analytics (STA) | Application Server (BSAFE Crypto-J) | HTTPS | Sí | 9.8 |
| CVE-2020-35168 | Oracle StorageTek Tape Analytics (STA) | Application Server (Dell BSAFE Micro Edition Suite) | HTTPS | Sí | 9.8 |
| CVE-2024-20999 | Oracle Solaris | Zones | NaN | No | 8.2 |
| CVE-2024-21059 | Oracle Solaris | Utility | NaN | No | 7.8 |
| CVE-2022-42890 | Oracle Solaris Cluster | Tools (Apache Batik) | HTTP | Sí | 7.5 |
| CVE-2023-24998 | Oracle Solaris Cluster | Tools (Apache Commons FileUpload) | HTTP | Sí | 7.5 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2022-45688 | Oracle Solaris Cluster | Tools (JSON-java) | HTTP | Sí | 7.5 |
| CVE-2023-1436 | Oracle Solaris Cluster | Tools (Jettison) | HTTP | Sí | 7.5 |
| CVE-2022-24839 | Oracle Solaris Cluster | Tools (NekoHTML) | HTTP | Sí | 7.5 |
| CVE-2022-42003 | Oracle Solaris Cluster | Tools (jackson-databind) | HTTP | Sí | 7.5 |
| CVE-2023-1370 | Oracle Solaris Cluster | Tools (json-smart) | HTTP | Sí | 7.5 |
| CVE-2023-1436 | Oracle StorageTek Tape Analytics (STA) | Application Server (Jettison) | HTTP | Sí | 7.5 |
| CVE-2022-24839 | Oracle StorageTek Tape Analytics (STA) | Core (NekoHTML) | HTTP | Sí | 7.5 |
| CVE-2021-37533 | Oracle Solaris Cluster | Tools (Apache Commons Net) | HTTP | Sí | 6.5 |
| CVE-2023-20863 | Oracle Solaris Cluster | Tools (Spring Framework) | HTTP | No | 6.5 |
| CVE-2024-21104 | Oracle ZFS Storage Appliance Kit | Core | NaN | No | 6.5 |
| CVE-2022-36033 | Oracle Solaris Cluster | Tools (jsoup) | HTTP | Sí | 6.1 |
| CVE-2021-36374 | Oracle Solaris Cluster | Tools (Apache Ant) | NaN | No | 5.5 |
| CVE-2023-1370 | Oracle StorageTek Tape | Core (json-smart) | HTTP | Sí | 5.3 |

| | | | | | |
|---|---|---|---|---|---|
| | Analytics (STA) | | | | |
| CVE-2024-21105 | Oracle Solaris | Utility | NaN | No | 2.0 |

## Matriz de riesgos de Oracle Utilities Applications

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2020-25638 | Oracle Utilities Application Framework | General (hibernate-core) | HTTP | Sí | 7.4 |
| CVE-2023-44487 | Oracle Utilities Network Management System | Monitoring: High Availability (Netty) | HTTP | Sí | 5.3 |

## Matriz de riesgos de Oracle Virtualization

| CVE ID | Componente | Privilegios requeridos | Protocolo | Explotación remota sin autorización | CVSS |
|---|---|---|---|---|---|
| CVE-2024-21112 | Oracle VM VirtualBox | Core | NaN | No | 8.8 |
| CVE-2024-21113 | Oracle VM VirtualBox | Core | NaN | No | 8.8 |
| CVE-2024-21114 | Oracle VM VirtualBox | Core | NaN | No | 8.8 |
| CVE-2024-21115 | Oracle VM VirtualBox | Core | NaN | No | 8.8 |
| CVE-2024-21103 | Oracle VM VirtualBox | Core | NaN | No | 7.8 |
| CVE-2024-21111 | Oracle VM VirtualBox | Core | NaN | No | 7.8 |
| CVE-2024-21116 | Oracle VM VirtualBox | Core | NaN | No | 7.8 |

| | | | | | |
|---|---|---|---|---|---|
| CVE-2024-21110 | Oracle VM VirtualBox | Core | NaN | No | 7.3 |
| CVE-2024-21107 | Oracle VM VirtualBox | Core | NaN | No | 6.7 |
| CVE-2024-21106 | Oracle VM VirtualBox | Core | NaN | No | 6.5 |
| CVE-2024-21121 | Oracle VM VirtualBox | Core | NaN | No | 6.5 |
| CVE-2024-21109 | Oracle VM VirtualBox | Core | HTTP | Sí | 5.9 |
| CVE-2024-21108 | Oracle VM VirtualBox | Core | NaN | No | 3.3 |

## 4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, Oracle publica las actualizaciones de seguridad pertinentes junto con sus alertas de seguridad, las cuales están disponibles en Oracle Security Alerts.

## 5. Referencias Adicionales

- Oracle Critical Patch Update Advisory - April 2024.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY