Alerta de seguridad cibernética	9VSA23-00774-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2023
Última revisión	18 de enero de 2023

NOTIFICACIÓN

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

Resumen

El CSIRT de Gobierno comparte información sobre vulnerabilidades que afectan a varios productos de Oracle, que fueron parchadas y comunicadas por la empresa como parte de su actualización de seguridad de enero 2023 (Oracle Critical Patch Update Advisory - January 2023).

Vulnerabilidades

CVE-2018-1273	CVE-2021-3737	CVE-2022-22978	CVE-2022-31129
CVE-2018-25032	CVE-2021-37533	CVE-2022-23219	CVE-2022-31629
CVE-2018-7489	CVE-2021-3918	CVE-2022-23221	CVE-2022-31692
CVE-2019-12415	CVE-2021-40528	CVE-2022-23305	CVE-2022-3171
CVE-2019-17571	CVE-2021-41184	CVE-2022-23437	CVE-2022-31813
CVE-2019-7317	CVE-2021-41411	CVE-2022-23457	CVE-2022-32212
CVE-2020-10683	CVE-2021-42717	CVE-2022-24329	CVE-2022-32221
CVE-2020-10693	CVE-2021-43797	CVE-2022-24407	CVE-2022-33980
CVE-2020-10735	CVE-2021-44832	CVE-2022-24823	CVE-2022-34169
CVE-2020-11979	CVE-2021-45105	CVE-2022-24839	CVE-2022-34305
CVE-2020-11987	CVE-2022-0084	CVE-2022-24903	CVE-2022-34917
CVE-2020-13956	CVE-2022-0492	CVE-2022-2509	CVE-2022-3510
CVE-2020-16156	CVE-2022-0934	CVE-2022-25236	CVE-2022-35737
CVE-2020-27844	CVE-2022-1122	CVE-2022-2526	CVE-2022-36033
CVE-2020-36242	CVE-2022-1304	CVE-2022-25315	CVE-2022-36055
CVE-2020-36518	CVE-2022-1319	CVE-2022-25647	CVE-2022-37434
CVE-2021-23358	CVE-2022-1941	CVE-2022-25857	CVE-2022-37454
CVE-2021-2351	CVE-2022-2048	CVE-2022-26336	CVE-2022-38752
CVE-2021-29425	CVE-2022-2053	CVE-2022-27404	CVE-2022-39271
CVE-2021-31805	CVE-2022-21824	CVE-2022-27782	CVE-2022-39429
CVE-2021-31812	CVE-2022-2274	CVE-2022-29824	CVE-2022-40146
CVE-2021-36090	CVE-2022-22965	CVE-2022-30126	CVE-2022-40149
CVE-2021-36483	CVE-2022-22970	CVE-2022-3028	CVE-2022-40150
CVE-2021-36770	CVE-2022-22971	CVE-2022-30293	CVE-2022-40153

CONTACTO Y REDES SOCIALES DEL CSIRT DE GOBIERNO
https://www.csirt.gob.cl
Teléfonos: 1510 | + (562) 24863850 | Correo: soc-csirt@interior.gob.cl
@csirtgob
https://www.linkedin.com/company/csirt-gob

CVE-2022-40304	CVE-2023-21835	CVE-2023-21859	CVE-2023-21883
CVE-2022-40664	CVE-2023-21836	CVE-2023-21860	CVE-2023-21884
CVE-2022-4147	CVE-2023-21837	CVE-2023-21861	CVE-2023-21885
CVE-2022-41720	CVE-2023-21838	CVE-2023-21862	CVE-2023-21886
CVE-2022-41881	CVE-2023-21839	CVE-2023-21863	CVE-2023-21887
CVE-2022-42003	CVE-2023-21840	CVE-2023-21864	CVE-2023-21888
CVE-2022-42252	CVE-2023-21841	CVE-2023-21865	CVE-2023-21889
CVE-2022-42889	CVE-2023-21842	CVE-2023-21866	CVE-2023-21890
CVE-2022-42915	CVE-2023-21843	CVE-2023-21867	CVE-2023-21891
CVE-2022-42920	CVE-2023-21844	CVE-2023-21868	CVE-2023-21892
CVE-2022-43403	CVE-2023-21845	CVE-2023-21869	CVE-2023-21893
CVE-2022-43548	CVE-2023-21846	CVE-2023-21870	CVE-2023-21894
CVE-2022-43680	CVE-2023-21847	CVE-2023-21871	CVE-2023-21898
CVE-2022-45047	CVE-2023-21848	CVE-2023-21872	CVE-2023-21899
CVE-2023-21824	CVE-2023-21849	CVE-2023-21873	CVE-2023-21900
CVE-2023-21825	CVE-2023-21850	CVE-2023-21874	CVE-2021-21708
CVE-2023-21826	CVE-2023-21851	CVE-2023-21875	CVE-2022-2047
CVE-2023-21827	CVE-2023-21852	CVE-2023-21876	CVE-2022-21597
CVE-2023-21828	CVE-2023-21853	CVE-2023-21877	CVE-2022-2191
CVE-2023-21829	CVE-2023-21854	CVE-2023-21878	CVE-2022-22950
CVE-2023-21830	CVE-2023-21855	CVE-2023-21879	CVE-2022-38749
CVE-2023-21831	CVE-2023-21856	CVE-2023-21880	CVE-2022-38750
CVE-2023-21832	CVE-2023-21857	CVE-2023-21881	CVE-2022-38751
CVE-2023-21834	CVE-2023-21858	CVE-2023-21882	CVE-2022-42004

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-2274: Vulnerabilidad fácil de explotar, existente en el componente Essbase Web Platform (OpenSSL) de Oracle Essbase 21.4, en el producto Siebel CRM de Oracle Siebel CRM 22.10. Permite a un atacante no autenticado con acceso de red via HTTPS comprometer Oracle Essbase o Oracle Siebel CRM 22.1.0, según corresponda.

CVE-2022-22965: Vulnerabilidad en el producto Oracle Commerce Guided Search de Oracle Commerce 11.3.2. Vulnerabilidad fácil de explotar que permite a un atacante no autenticado con acceso de red via HTTP comprometer Oracle Commerce Guided Search.

CVE-2022-42889: Vulnerabilidad en varios productos de Oracle Communications Applications, Oracle Fusion Middleware, Oracle Hyperion, Oracle JD Edwards, Oracle Utilities Applications y Oracle Database Server. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer aquellos productos.

CVE-2022-33980: Vulnerabilidad fácil de explotar que permite a un atacante no autenticado con acceso de red via HTTP comprometer varios productos de Oracle Financial Services Applications, al producto Oracle Communications Elastic Charging Engine de Oracle Communications Applications 12.0.0.5.0-

12.0.0.7.0, los productos Oracle Banking Party Management, Oracle Financial Services Crime and Compliance Management Studio y Oracle Banking Enterprise Default Management de Oracle Financial Services Applications 2.7.0. y al producto Oracle Communications Elastic Charging Engine de Oracle Communications Application 12.0.0.5.0-12.0.0.7.0. y 8.0.8.3.1. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer los respectivos productos mencionados.

CVE-2019-17571: Vulnerabilidad en el producto Oracle Communications Unified Assurance de Oracle Communications Applications 5.5.0-5.5.9 y 6.0.0-6.0.1. Fácil de explotar, permite a un atacante no autenticado con acceso de red a través de HTTPS comprometer Oracle Communications Unified Assurance.

CVE-2022-22978: Vulnerabilidad en el producto Oracle Communications Unified Assurance de Oracle Communications Applications 5.5.0-5.5.9 y 6.0.0-6.0.1. Fácil de explotar, permite a un atacante no autenticado con acceso de red a través de HTTPS comprometer Oracle Communications Unified Assurance.

CVE-2022-37454: Vulnerabilidad en el producto Oracle Communications Unified Assurance de Oracle Communications Applications 5.5.0-5.5.9. Fácil de explotar, permite a un atacante no autenticado con acceso de red a través de HTTPS comprometer Oracle Communications Unified Assurance.

CVE-2022-31692: Vulnerabilidad en productos de Oracle Communications 22.3.0 y 22.3.1 y en el producto MySQL Enterprise Monitor de Oracle MySQL 8.0.32 y anteriores. Fácil de explotar, permite a un atacante no autenticado con acceso de red a través de HTTPS comprometer productos de Oracle Communications y MySQL Enterprise Monitor.

CVE-2021-41411: Vulnerabilidad en el producto Oracle Communications Unified Inventory Management de Oracle Communications Applications 7.4.0, 7.4.1, 7.4.2 y 7.5.0. Fácil de explotar, permite a un atacante no autenticado con acceso de red a través de HTTPS comprometer productos de Oracle Communications Unified Inventory Management.

CVE-2022-43403: Vulnerabilidad en el producto Oracle Communications Cloud Native Core Unified Data Repository de Oracle Communications 22.3.3. Fácil de explotar, permite a un atacante con bajos privilegios y acceso de red a través de HTTPS comprometer a Oracle Communications Cloud Native Core Unified Data Repository.

CVE-2022-2526: Vulnerabilidad en el producto Oracle Communications Cloud Native Core Automated Test Suite de Oracle Communications 22.2.2, 22.3.1 y 22.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Communications Cloud Native Core Automated Test Suite.

CVE-2022-27404: Vulnerabilidad en varios productos de Oracle Communications 22.2.1 y 22.3.0, y Oracle Fusion Middleware 8.5.6. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Communications y Oracle Fusion Middleware.

CVE-2022-25315: Vulnerabilidad en el producto Oracle Communications Cloud Native Core Binding Support Function de Oracle Communications 22.2.4. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Communications.

CVE-2022-42915: Vulnerabilidad en el producto Oracle Communications Cloud Native Core Binding Support Function de Oracle Communications 22.1.1. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Communications Cloud Native Core Binding Support Function

CVE-2022-37434: Vulnerabilidad en el producto Oracle Communications Cloud Native Core Binding Support Function de Oracle Communications 22.1.1, el producto Oracle Communications Cloud Native Core Security Edge Protection Proxy de Oracle Communications 22.3.1, el producto Oracle Communications Diameter Signaling Router de Oracle Communications 8.6.0.0, el producto Oracle Outside In Technology de Oracle Fusion Middleware 8.5.6, el producto MySQL Workbench de Oracle MySQL 8.0.31, el producto PeopleSoft Enterprise PeopleTools product de Oracle PeopleSoft 8.58, 8.59 y 8.60 y en Oracle TimesTen In-Memory Database, versiones anteriores a la 11.2.2.8.65. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer los respectivos productos mencionados.

CVE-2018-1273: Vulnerabilidad en los productos Oracle Communications Cloud Native Core Binding Support Function de Oracle Communications 22.2.0 y Oracle Healthcare Data Repository de Oracle HealthCare Applications 8.1.0.0-8.1.3.1. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer los respectivos productos mencionados.

CVE-2022-45047: Vulnerabailidad en el producto Oracle Coherence de Oracle Fusion Middleware 14.1.1.0.0, Oracle Global Lifecycle Management NextGen OUI Framework de Oracle Fusion Middleware 13.9.4.2.11, Middleware Common Libraries and Tools de Oracle Fusion Middleware 12.2.1.4.0 y 14.1.1.0.0, y en los productos OSS Support Tools product de Oracle Support Tools 2.12.43, 22.4.22.10.18 y 22.2.22.4.5. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía SSH o HTTPS (dependiendo del producto), pueda comprometer aquellos productos.

CVE-2022-23305: Vulnerabilidad en el producto Oracle Coherence de Oracle Fusion Middleware 12.2.1.3.0 and 12.2.1.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Coherence.

CVE-2022-25236: Vulnerabilidad en el producto Oracle HTTP Server de Oracle Fusion Middleware 12.2.1.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle HTTP Server.

CVE-2022-31813: Vulnerabilidad en el producto Oracle HTTP Server de Oracle Fusion Middleware 12.2.1.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle HTTP Server.
CVE-2022-40664: Vulnerabilidad en el producto Oracle WebCenter Sites de Oracle Fusion Middleware 12.2.1.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle WebCenter Sites.

CVE-2018-7489: Vulnerabilidad en el producto Oracle WebLogic Server de Oracle Fusion Middleware 12.2.1.3.0, 12.2.1.4.0 y 14.1.1.0.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle WebLogic Server.

CVE-2022-42920: Vulnerabilidad en el producto Oracle WebLogic Server de Oracle Fusion Middleware 12.2.1.3.0 y 12.2.1.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle WebLogic Server.

CVE-2022-23457: Vulnerabilidad en el producto Oracle Health Sciences Empirica Signal de Oracle Health Sciences Applications 9.1.0.52 y 9.2.0.52 y el producto Oracle Middleware Common Libraries and Tools de Oracle Fusion Middleware 12.2.1.4.0. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Health Sciences Empirica Signal y Oracle Middleware Common Libraries and Tools.

CVE-2022-23221: Vulnerabilidad en el producto Oracle Healthcare Translational Research de Oracle HealthCare Applications 4.1.0.0-4.1.1.1. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Healthcare Translational Research.

CVE-2021-31805: Vulnerabilidad en el producto Oracle Hyperion Infrastructure Technology de Oracle Hyperion 11.2.10. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Hyperion Infrastructure Technology.

CVE-2022-32221: Vulnerabilidad en el producto Oracle MySQL Server de Oracle MySQL 5.7.40 y anteriores y 8.0.31 y anteriores. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a MySQL Server.

CVE-2020-36242: Vulnerabilidad en el producto MySQL Shell product de Oracle MySQL 8.0.31. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía múltiples protocolos pueda comprometer a MySQL Shell.

CVE-2021-3918: Vulnerabilidad en el producto PeopleSoft Enterprise CC Common Application Objects de Oracle PeopleSoft 9.2. y el producto PeopleSoft Enterprise PeopleTools de Oracle PeopleSoft 8.58, 8.59 y 8.60. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a PeopleSoft Enterprise CC Common Application Objects y PeopleSoft Enterprise PeopleTools.

CVE-2022-23219: Vulnerabilidad en el producto Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers de Oracle Systems anteriores a XCP2411, XCP3111 y XCP4011. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers

CVE-2020-10683: Vulnerabilidad en el producto Oracle Utilities Network Management System de Oracle Utilities Applications 2.3.0.2, 2.4.0.1, 2.5.0.0, 2.5.0.1 y 2.5.0.2. Fácil de explotar, permite que un atacante no autenticado, con acceso de red vía HTTPS, pueda comprometer a Oracle Utilities Network Management System.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Enterprise Manager Base Platform13.4.0.0, 13.5.0.0
Enterprise Manager Ops Center12.4.0.0
Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S ServersPrior to XCP2411, prior to XCP3111, prior to XCP4011
GoldenGate Stream AnalyticsPrior to 19.1.0.0.8
Java VM19c, 21c
JD Edwards EnterpriseOne OrchestratorPrior to 9.2.7.2
JD Edwards EnterpriseOne ToolsPrior to 9.2.7.2
Management Cloud Engine22.1.0.0.0
Middleware Common Libraries and Tools12.2.1.4.0, 14.1.1.0.0
MySQL Cluster7.4.38 and prior,7.5.28 and prior,7.6.24 and prior, 8.0.31 and prior
MySQL Connectors8.0.31 and prior
MySQL Enterprise Monitor8.0.32 and prior
MySQL Server5.7.40 and prior
MySQL Server5.7.40 and prior, 8.0.31 and prior
MySQL Server8.0.28 and prior
MySQL Server8.0.29 and prior
MySQL Server8.0.30 and prior
MySQL Server8.0.31 and prior
MySQL Shell8.0.31 and prior
MySQL Workbench8.0.31 and prior
Oracle Access Manager12.2.1.4.0
Oracle Agile PLM9.3.6
Oracle Applications DBA12.2.3-12.2.12
Oracle AutoVuePrior to 21.0.2.0
Oracle AutoVuePrior to 21.0.2.6
Oracle Banking Enterprise Default Management2.6.2
Oracle Banking Enterprise Default Management2.7.0
Oracle Banking Enterprise Default Management2.7.1, 2.12.0
Oracle Banking Loans Servicing2.8.0, 2.12.0
Oracle Banking Party Management2.7.0
Oracle Banking Platform2.6.2, 2.7.1, 2.9.0, 2.12.0
Oracle BI Publisher5.9.0.0.0, 6.4.0.0.0, 12.2.1.4.0
Oracle Business Intelligence Enterprise Edition5.9.0.0.0, 6.4.0.0.0
Oracle Coherence12.2.1.3.0, 12.2.1.4.0
Oracle Coherence14.1.1.0.0
Oracle Collaborative Planning12.2.3-12.2.12
Oracle Commerce Guided Search11.3.2
Oracle Communications Billing and Revenue Management12.0.0.4.0-12.0.0.7.0
Oracle Communications BRM - Elastic Charging Engine12.0.0.3.0-12.0.0.7.0
Oracle Communications Calendar Server8.0.0.6.0
Oracle Communications Cloud Native Core Automated Test Suite22.2.2, 22.3.1, 22.4.0

Oracle Communications Cloud Native Core Binding Support Function22.1.0, 22.2.0
Oracle Communications Cloud Native Core Binding Support Function22.1.1
Oracle Communications Cloud Native Core Binding Support Function22.2.0
Oracle Communications Cloud Native Core Binding Support Function22.2.0, 22.2.2, 22.3.1
Oracle Communications Cloud Native Core Binding Support Function22.2.1
Oracle Communications Cloud Native Core Binding Support Function22.2.2
Oracle Communications Cloud Native Core Binding Support Function22.2.4
Oracle Communications Cloud Native Core Binding Support Function22.3.0
Oracle Communications Cloud Native Core Binding Support Function22.3.0-22.4.0
Oracle Communications Cloud Native Core Binding Support Function22.3.2, 22.2.0
Oracle Communications Cloud Native Core Console22.3.0
Oracle Communications Cloud Native Core Console22.3.0, 22.4.0
Oracle Communications Cloud Native Core Network Data Analytics Function22.0.0.0.0
Oracle Communications Cloud Native Core Network Exposure Function22.3.1
Oracle Communications Cloud Native Core Network Exposure Function22.3.1, 22.4.0
Oracle Communications Cloud Native Core Network Function Cloud Native Environment22.3.0
Oracle Communications Cloud Native Core Network Repository Function22.3.0
Oracle Communications Cloud Native Core Network Repository Function22.3.2
Oracle Communications Cloud Native Core Network Slice Selection Function22.3.1
Oracle Communications Cloud Native Core Network Slice Selection Function22.3.1, 22.4.1
Oracle Communications Cloud Native Core Policy1.11.0
Oracle Communications Cloud Native Core Policy22.3.0
Oracle Communications Cloud Native Core Policy22.3.0, 22.4.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy22.3.1
Oracle Communications Cloud Native Core Security Edge Protection Proxy22.4.0, 22.3.1
Oracle Communications Cloud Native Core Unified Data Repository22.2.2, 22.3.3
Oracle Communications Cloud Native Core Unified Data Repository22.3.3
Oracle Communications Cloud Native Core Unified Data Repository22.3.3, 22.4.0
Oracle Communications Cloud Native Core Unified Data Repository22.3.4, 22.2.3
Oracle Communications Contacts Server8.0.0.7.0
Oracle Communications Converged Application Server7.1.0, 8.0.0
Oracle Communications Convergence3.0.3.1.0
Oracle Communications Design Studio7.4.2
Oracle Communications Diameter Intelligence Hub8.2.3.0
Oracle Communications Diameter Signaling Router8.6.0.0
Oracle Communications Elastic Charging Engine12.0.0.3.0-12.0.0.7.0
Oracle Communications Elastic Charging Engine12.0.0.5.0-12.0.0.7.0
Oracle Communications Instant Messaging Server10.0.1.6.0
Oracle Communications Messaging Server8.1.0.20.0
Oracle Communications MetaSolv Solution6.3.1
Oracle Communications Order and Service Management7.4.0
Oracle Communications Performance Intelligence Center (PIC) Software10.4.0.4.1
Oracle Communications Pricing Design Center12.0.0.5.0-12.0.0.7.0
Oracle Communications Unified Assurance5.5.0-5.5.9
Oracle Communications Unified Assurance5.5.0-5.5.9, 6.0.0-6.0.1
Oracle Communications Unified Inventory Management7.4.0, 7.4.1, 7.4.2

Oracle Communications Unified Inventory Management7.4.0, 7.4.1, 7.4.2, 7.5.0
Oracle Communications Unified Inventory Management7.4.0-7.4.2, 7.5.0
Oracle Communications Unified Inventory Management7.5.0
Oracle Data Provider for .NET19c, 21c
Oracle Database - Machine Learning for Python (Python)21c
Oracle Database - Workload Manager (jackson-databind)21c
Oracle Database (Python)21c
Oracle Database (zlib)19c, 21c
Oracle Database Data Redaction19c, 21c
Oracle Database Fleet Patching (jackson-databind)21c
Oracle Database RDBMS Security19c, 21c
Oracle Demantra Demand Management12.1, 12.2
Oracle Demantra Demand Management12.2.7, 12.2.8, 12.2.9, 12.2.10, 12.2.11, 12.2.12
Oracle Documaker12.4.0-12.7.0
Oracle Essbase21.4
Oracle Financial Services Crime and Compliance Management Studio8.0.8.3.1
Oracle Fusion Middleware MapViewer12.2.1.4.0
Oracle Global Lifecycle Management NextGen OUI FrameworkPrior to 13.9.4.2.11
Oracle GraalVM Enterprise EditionOracle GraalVM Enterprise Edition: 20.3.8, 21.3.4, 22.3.0
Oracle HCM Common Architecture12.2.3-12.2.12
Oracle Health Sciences Empirica Signal9.1.0.52, 9.2.0.52
Oracle Healthcare Data Repository8.1.0.0-8.1.3.1
Oracle Healthcare Translational Research4.1.0.0-4.1.1.1
Oracle Hospitality Cruise Shipboard Property Management System20.2.2
Oracle Hospitality Gift and Loyalty9.1.0
Oracle Hospitality Labor Management9.1.0
Oracle Hospitality Reporting and Analytics9.1.0
Oracle Hospitality Simphony18.2.11, 19.3.4
Oracle HTTP Server12.2.1.4.0
Oracle Hyperion Infrastructure Technology11.2.10
Oracle iSetup12.2.3-12.2.12
Oracle iSupplier Portal12.2.6-12.2.8
Oracle Java SE, Oracle GraalVM Enterprise EditionOracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4, 22.3.0
Oracle Java SE, Oracle GraalVM Enterprise EditionOracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4, 22.3.0
Oracle Java SE, Oracle GraalVM Enterprise EditionOracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4
Oracle Learning Management12.2.3-12.2.12
Oracle Marketing12.2.3-12.2.12
Oracle Middleware Common Libraries and Tools12.2.1.4.0
Oracle Mobile Field Service12.2.3-12.2.12
Oracle Outside In Technology8.5.6
Oracle Retail Service Backbone14.1.3.2, 15.0.3.1, 16.0.3
Oracle Sales for Handhelds12.2.3-12.2.12
Oracle Sales Offline12.2.3-12.2.12

Oracle Self-Service Human Resources12.2.3-12.2.12
Oracle Solaris10, 11
Oracle Stream AnalyticsPrior to 19.1.0.0.8
Oracle TimesTen In-Memory DatabasePrior to 11.2.2.8.65
Oracle Utilities Framework4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.5.0.0.0
Oracle Utilities Framework4.4.0.3.0, 4.5.0.0.0
Oracle Utilities Network Management System2.3.0.2, 2.4.0.1, 2.5.0.0, 2.5.0.1, 2.5.0.2
Oracle Utilities Network Management System2.3.0.2, 2.4.0.1, 2.5.0.0-2.5.0.2
Oracle Utilities Network Management System2.5.0.1, 2.5.0.2
Oracle VM VirtualBoxPrior to 6.1.42, prior to 7.0.6
Oracle Web Applications Desktop Integrator12.2.3-12.2.12
Oracle Web Services Manager12.2.1.4.0
Oracle WebCenter Content12.2.1.4.0
Oracle WebCenter Sites12.2.1.4.0
Oracle WebLogic Server12.2.1.3.0, 12.2.1.4.0
Oracle WebLogic Server12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
Oracle WebLogic Server14.1.1.0.0
OSS Support Tools2.12.43
OSS Support Tools22.2.22.4.5
OSS Support Tools22.4.22.10.18
PeopleSoft Enterprise CC Common Application Objects9.2
PeopleSoft Enterprise CS Academic Advisement9.2
PeopleSoft Enterprise PeopleTools8.58
PeopleSoft Enterprise PeopleTools8.58, 8.59, 8.60
PeopleSoft Enterprise PeopleTools8.59, 8.60
PeopleSoft Enterprise PeopleTools8.60
Primavera Gateway18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10, 21.12.0-21.12.8
Primavera Unifier18.8, 19.12, 20.12, 21.12, 22.12
ProductSupported Versions Affected
Siebel Apps - Marketing22.10 and prior
Siebel CRM22.10 and prior

Enlaces

https://www.oracle.com/security-alerts/cpujan2023.html
https://www.oracle.com/security-alerts/cpujan2023verbose.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1273
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7489
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17571
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7317
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10683
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10693
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10735
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11979
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11987

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16156
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27844
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36242
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23358
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2351
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31805
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31812
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36483
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36770
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3918
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41411
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42717
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0084
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0934
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1122
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1304
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1304
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1941
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2053
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2274
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22970
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22971
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22978
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23221
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23437
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23457
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24329
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24407
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24823

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24839
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24903
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25236
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25315
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26336
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27404
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27782
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30126
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3028
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30293
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31129
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31629
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31692
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3171
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32212
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32221
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34917
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-35737
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37454
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38752
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40146
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40149
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40150
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40153
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40304
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40664
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4147
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41720
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41881
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42003
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42252

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42915
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42920
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-43403
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-43548
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-43680
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21825
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21826
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21828
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21829
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21831
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21834
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21836
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21837
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21838
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21839
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21840
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21841
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21842
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21843
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21844
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21845
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21846
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21847
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21848
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21849
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21850
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21851
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21853
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21854
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21855
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21856
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21857
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21858
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21860
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21862
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21863

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21864
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21865
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21866
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21867
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21868
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21869
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21870
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21871
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21872
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21873
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21874
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21875
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21876
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21877
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21878
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21879
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21880
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21881
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21882
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21883
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21884
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21885
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21886
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21887
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21888
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21889
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21892
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21893
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21894
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21899
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21900
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21597
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2191
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-38751
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42004

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.18 17:03:00 -03'00'