Alerta de seguridad cibernética	9VSA24-00960-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2024
Última revisión	18 de enero de 2024

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 de vulnerabilidades parchadas por Oracle como parte de su Critical Patch Update (CPU) de enero de 2024.

Vulnerabilidades

CVE-2023-3823	CVE-2021-42575	CVE-2022-3602	CVE-2023-1108
CVE-2019-10086	CVE-2021-43306	CVE-2022-36033	CVE-2023-1370
CVE-2020-15250	CVE-2021-43527	CVE-2022-36944	CVE-2023-1436
CVE-2020-26870	CVE-2021-46848	CVE-2022-37434	CVE-2023-20883
CVE-2020-5410	CVE-2022-1471	CVE-2022-40152	CVE-2023-21833
CVE-2020-5421	=CVE-2022-22950	CVE-2022-40896	CVE-2023-21901
CVE-2020-7760	CVE-2022-22969	CVE-2022-41704	CVE-2023-21949
CVE-2021-0341	CVE-2022-22979	CVE-2022-42003	CVE-2023-22102
CVE-2021-29425	CVE-2022-23221	CVE-2022-42004	CVE-2023-2283
CVE-2021-33813	CVE-2022-24839	CVE-2022-42890	CVE-2023-23931
CVE-2021-35515	CVE-2022-25147	CVE-2022-42920	CVE-2023-24998
CVE-2021-35516	CVE-2022-25647	CVE-2022-4304	CVE-2023-25194
CVE-2021-35517	CVE-2022-29155	CVE-2022-4450	CVE-2023-2617
CVE-2021-36090	CVE-2022-31147	CVE-2022-44729	CVE-2023-2618
CVE-2021-36090	CVE-2022-31160	CVE-2022-44730	CVE-2023-2650
CVE-2021-37533	CVE-2022-31690	CVE-2022-45868	CVE-2023-27391
CVE-2021-4104	CVE-2022-31692	CVE-2022-46751	CVE-2023-28439
CVE-2021-41182	CVE-2022-33879	CVE-2022-46908	CVE-2023-28484
CVE-2021-41183	CVE-2022-34169	CVE-2022-48174	CVE-2023-28755
CVE-2021-41184	CVE-2022-3479	CVE-2023-0465	CVE-2023-28756
CVE-2021-42392	CVE-2022-3510	CVE-2023-0466	CVE-2023-28823

CVE-2023-29469
CVE-2023-2975
CVE-2023-2976
CVE-2023-30861
CVE-2023-31122
CVE-2023-31484
CVE-2023-31486
CVE-2023-31582
CVE-2023-32002
CVE-2023-32006
CVE-2023-32559
CVE-2023-32697
CVE-2023-33201
CVE-2023-34034
CVE-2023-34035
CVE-2023-34053
CVE-2023-34055
CVE-2023-34453
CVE-2023-34454
CVE-2023-34455
CVE-2023-3446
CVE-2023-34462
CVE-2023-34624
CVE-2023-34981
CVE-2023-35141
CVE-2023-35887
CVE-2023-36054
CVE-2023-3635
CVE-2023-36478
CVE-2023-36478
CVE-2023-36479
CVE-2023-36632
CVE-2023-37536
CVE-2023-3817
CVE-2023-3824
CVE-2023-38325
CVE-2023-38545
CVE-2023-38546
CVE-2023-39151
CVE-2023-39318
CVE-2023-39319
CVE-2023-39320
CVE-2023-39321
CVE-2023-39322
CVE-2023-39410
CVE-2023-39975
CVE-2023-40167
CVE-2023-41053
CVE-2023-41105
CVE-2023-41900
CVE-2023-42503
CVE-2023-42794
CVE-2023-42795
CVE-2023-43494
CVE-2023-43495
CVE-2023-43496
CVE-2023-43497
CVE-2023-43498
CVE-2023-43622
CVE-2023-43642
CVE-2023-43643
CVE-2023-44483
CVE-2023-44487
CVE-2023-44981
CVE-2023-45143
CVE-2023-45145
CVE-2023-45648
CVE-2023-45648.
CVE-2023-45802
CVE-2023-46589
CVE-2023-46604
CVE-2023-49093
CVE-2023-4911
CVE-2023-50164
CVE-2023-5072
CVE-2023-5363
CVE-2024-20904
CVE-2024-20905
CVE-2024-20906
CVE-2024-20907
CVE-2024-20908
CVE-2024-20909
CVE-2024-20910
CVE-2024-20911
CVE-2024-20912
CVE-2024-20913
CVE-2024-20914
CVE-2024-20915
CVE-2024-20916
CVE-2024-20917
CVE-2024-20918
CVE-2024-20919
CVE-2024-20920
CVE-2024-20921
CVE-2024-20922
CVE-2024-20923
CVE-2024-20924
CVE-2024-20925
CVE-2024-20926
CVE-2024-20927
CVE-2024-20928
CVE-2024-20929
CVE-2024-20930
CVE-2024-20931
CVE-2024-20932
CVE-2024-20933
CVE-2024-20934
CVE-2024-20935
CVE-2024-20936
CVE-2024-20937
CVE-2024-20938
CVE-2024-20939
CVE-2024-20940
CVE-2024-20941
CVE-2024-20942
CVE-2024-20943
CVE-2024-20944
CVE-2024-20945
CVE-2024-20946
CVE-2024-20947
CVE-2024-20948
CVE-2024-20949
CVE-2024-20950
CVE-2024-20951
CVE-2024-20952
CVE-2024-20953
CVE-2024-20955
CVE-2024-20956
CVE-2024-20957
CVE-2024-20958
CVE-2024-20959
CVE-2024-20960
CVE-2024-20961
CVE-2024-20962
CVE-2024-20963
CVE-2024-20964
CVE-2024-20965
CVE-2024-20966
CVE-2024-20967
CVE-2024-20968
CVE-2024-20969
CVE-2024-20970
CVE-2024-20971
CVE-2024-20972

CVE-2024-20973	CVE-2024-20977	CVE-2024-20981	CVE-2024-20985
CVE-2024-20974	CVE-2024-20978	CVE-2024-20982	CVE-2024-20986
CVE-2024-20975	CVE-2024-20979	CVE-2024-20983	CVE-2024-20987
CVE-2024-20976	CVE-2024-20980	CVE-2024-20984	

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2023-38545: Vulnerabilidad en el componente Essbase Web Platform (curl) de Oracle Essbase. CVSS: 9.8.

CVE-2022-36944: Vulnerabilidad de deserialización de Java en Scala 2.13.x anteriores al 2.13.9, que permite ejecución de código. CVSS: 9.8.

CVE-2022-42920: Vulnerabilidad por un error de escritura fuera de límites de la memoria en API de Apache Commons BCEL anterior a 6.6.0. CVSS: 9.8.

CVE-2022-1471: Vulnerabilidad en la clase Constructor de SnakeYaml que no restringe los tipos que pueden ser instanciados durante la deserialización. CVSS: 9.8.

CVE-2023-34034: Vulnerabilidad en la configuración Spring Security para WebFlux, que posibilita una evasión de seguridad. CVSS: 9.8.

CVE-2023-44981: Bypass de autorización dada una vulnerabilidad en Apache ZooKeeper. CVSS: 9.1.

CVE-2022-48174: Vulnerabilidad de stack overflow en ash.c:6030 en busybox anterior a 1.35. CVSS: 9.8.

CVE-2023-46604: Vulnerabilidad debida a un protocolo vulnerable a ejecución remota de código en Java OpenWire. CVSS: 9.8.

CVE-2023-50164: Vulnerabilidad en Struts anterior a 2.5.33 o 6.3.0.2 que permite cargar un archivo malicioso que puede ser usado para ejecución remota de código. CVSS: 9.8.

CVE-2021-46848: GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der. CVSS: 9.1

CVE-2022-31692: Vulnerabilidad en Spring Security 5.7 anteriores a 5.7.5 y 5.6 anteriores a 5.6.9, susceptibles a bypass de las reglas de autenticación. CVSS: 9.8.

CVE-2023-38545: Vulnerabilidad de heap buffer overflow en el handshake proxy SOCKS5. CVSS: 9.8.

CVE-2022-23221: Vulnerabilidad en la H2 Console anteriores del 2.1.210 permite a atacantes remotos ejecutar código arbitrario. CVSS: 9.8.

CVE-2022-37434: Vulnerabilidad en zlib hasta el 1.2.12. CVSS: 9.8.

CVE-2021-42575: Vulnerabilidad en OWASP Java HTML, no hay aplicación correcta de las políticas de los elementos SELECT, STYLE y OPTION. CVSS: 9.8.

CVE-2023-32002: Vulnerabilidad en Node.js en productos NetApp. CVSS: 9.8.

CVE-2023-50164: Vulnerabilidad en Struts anteriores a 2.5.33 y 6.3.0.2 que permite manipular parámetros de carga de archivos que permite paths traversal y ejecución remota de código. CVSS: 9.8.

CVE-2022-29155: Vulnerabilidad de inyección SQL en QpenLDAP 2.x anteriores a 2.5.12 y 2.6.x anterior a 2.6.2. CVSS: 9.8

CVE-2021-43527: Versiones anteriores a 3.63 o 3.68.1 de NSS ESR son vulnerables a un heap overflow al manipular firmas DSA encodeadas con DER, o RSA-PSS. CVSS: 9.8.

Mitigación

Implementar el CPU de enero 2024. Más información para clientes Oracle:
https://support.oracle.com/rs?type=doc&id=2980981.1

Productos afectados

Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers
Graph Server and Client
Integrated Lights Out Manager (ILOM)
JD Edwards EnterpriseOne Orchestrator
JD Edwards EnterpriseOne Tools
MySQL Cluster
MySQL Connectors
MySQL Enterprise Monitor
MySQL Server
MySQL Workbench
Oracle Access Manager
Oracle Agile PLM
Oracle Agile Product Lifecycle Management for Process
Oracle Analytics Desktop
Oracle Application Object Library
Oracle Application Testing Suite
Oracle Audit Vault and Database Firewall
Oracle Banking APIs
Oracle Banking Branch

Oracle Banking Cash Management
Oracle Banking Collections and Recovery
Oracle Banking Corporate Lending Process Management
Oracle Banking Credit Facilities Process Management
Oracle Banking Digital Experience
Oracle Banking Electronic Data Exchange for Corporates
Oracle Banking Enterprise Default Management
Oracle Banking Extensibility Workbench
Oracle Banking Liquidity Management
Oracle Banking Origination
Oracle Banking Party Management
Oracle Banking Supply Chain Finance
Oracle Banking Trade Finance Process Management
Oracle Banking Virtual Account Management
Oracle BI Publisher
Oracle Big Data Spatial and Graph
Oracle Business Intelligence Enterprise Edition
Oracle Business Process Management Suite
Oracle Coherence
Oracle Commerce Guided Search
Oracle Commerce Platform
Oracle Common Applications
Oracle Communications ASAP
Oracle Communications Billing and Revenue Management
Oracle Communications BRM - Elastic Charging Engine
Oracle Communications Cloud Native Core Automated Test Suite
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 Security Edge Protection Proxy
Oracle Communications Cloud Native Core Unified Data Repository
Oracle Communications Convergence
Oracle Communications Convergent Charging Controller
Oracle Communications Diameter Signaling Router
Oracle Communications Element Manager
Oracle Communications Fraud Monitor
Oracle Communications Instant Messaging Server
Oracle Communications IP Service Activator
Oracle Communications Messaging Server
Oracle Communications MetaSolv Solution
Oracle Communications Network Analytics Data Director

Oracle Communications Network Charging and Control
Oracle Communications Order and Service Management
Oracle Communications Policy Management
Oracle Communications Pricing Design Center
Oracle Communications Service Catalog and Design
Oracle Communications Session Report Manager
Oracle Communications Unified Assurance
Oracle Communications Unified Inventory Management
Oracle Complex Maintenance, Repair, and Overhaul
Oracle CRM Technical Foundation
Oracle Customer Interaction History
Oracle Enterprise Data Quality
Oracle Enterprise Manager Base Platform
Oracle Enterprise Manager for Fusion Middleware
Oracle Enterprise Manager for Oracle Database
Oracle Enterprise Manager for Oracle Virtual Infrastructure
Oracle Enterprise Manager for Virtualization
Oracle Enterprise Manager Ops Center
Oracle Essbase
Oracle Financial Services Analytical Applications Infrastructure
Oracle Financial Services Behavior Detection Platform
Oracle Financial Services Compliance Studio
Oracle Financial Services Enterprise Case Management
Oracle Financial Services Lending and Leasing
Oracle Financial Services Revenue Management and Billing
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition
Oracle FLEXCUBE Enterprise Limits and Collateral Management
Oracle FLEXCUBE Investor Servicing
Oracle FLEXCUBE Private Banking
Oracle Fusion Middleware
Oracle GoldenGate
Oracle GraalVM for JDK
Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition
Oracle HTTP Server
Oracle Hyperion Calculation Manager
Oracle Hyperion Financial Data Quality Management, Enterprise Edition
Oracle Hyperion Financial Management
Oracle Hyperion Financial Reporting
Oracle Hyperion Infrastructure Technology
Oracle Hyperion Planning
Oracle Identity Manager
Oracle Installed Base
Oracle iStore
Oracle iSupport

Oracle Java SE, Oracle GraalVM Enterprise Edition
Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition
Oracle JDeveloper
Oracle Knowledge Management
Oracle Managed File Transfer
Oracle Middleware Common Libraries and Tools
Oracle NoSQL Database
Oracle One-to-One Fulfillment
Oracle Outside In Technology
Oracle Retail Advanced Inventory Planning
Oracle Retail Customer Management and Segmentation Foundation
Oracle Retail EFTLink
Oracle Service Bus
Oracle SOA Suite
Oracle Solaris
Oracle Utilities Network Management System
Oracle Utilties Application Framework
Oracle Web Applications Desktop Integrator
Oracle WebCenter Content
Oracle WebCenter Portal
Oracle WebCenter Sites
Oracle WebLogic Server
Oracle ZFS Storage Appliance Kit
PeopleSoft Enterprise PeopleTools
Primavera P6 Enterprise Project Portfolio Management
Primavera Unifier
Product
Siebel CRM

Enlaces

https://www.oracle.com/security-alerts/cpujan2024.html

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.19 11:29:40 -03'00'