Alerta de seguridad cibernética	9VSA23-00868-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de julio de 2023
Última revisión	24 de julio 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 de las vulnerabilidades contenidas en el Oracle Critical Patch Update Advisory para julio de 2023, varias de ellas críticas.

Vulnerabilidades

CVE-2018-1282	CVE-2021-26117	CVE-2022-22950
CVE-2018-25032	CVE-2021-28168	CVE-2022-22971
CVE-2019-0227	CVE-2021-29425	CVE-2022-23305
CVE-2019-10086	CVE-2021-33813	CVE-2022-23437
CVE-2019-13990	CVE-2021-34429	CVE-2022-23491
CVE-2019-17531	CVE-2021-36090	CVE-2022-24409
CVE-2020-10735	CVE-2021-36374	CVE-2022-24891
CVE-2020-11988	CVE-2021-37533	CVE-2022-25147
CVE-2020-13936	CVE-2021-40528	CVE-2022-25647
CVE-2020-13956	CVE-2021-40690	CVE-2022-27404
CVE-2020-17521	CVE-2021-4104	CVE-2022-29361
CVE-2020-35168	CVE-2021-41183	CVE-2022-29546
CVE-2020-35169	CVE-2021-41184	CVE-2022-2963
CVE-2020-36518	CVE-2021-42575	CVE-2022-31129
CVE-2020-7760	CVE-2021-43113	CVE-2022-31160
CVE-2020-8908	CVE-2021-43859	CVE-2022-31197
CVE-2021-22569	CVE-2021-46877	CVE-2022-31692
CVE-2021-23926	CVE-2022-1122	CVE-2022-3171
CVE-2021-24112	CVE-2022-1471	CVE-2022-31777
CVE-2021-25220	CVE-2022-2048	CVE-2022-33879

CVE-2022-33980	CVE-2023-0767	CVE-2023-22027
CVE-2022-3479	CVE-2023-1370	CVE-2023-22031
CVE-2022-36033	CVE-2023-1436	CVE-2023-22033
CVE-2022-36944	CVE-2023-1999	CVE-2023-22034
CVE-2022-37434	CVE-2023-20860	CVE-2023-22035
CVE-2022-37865	CVE-2023-20861	CVE-2023-22036
CVE-2022-40150	CVE-2023-20862	CVE-2023-22037
CVE-2022-40152	CVE-2023-20863	CVE-2023-22038
CVE-2022-40897	CVE-2023-20873	CVE-2023-22039
CVE-2022-41853	CVE-2023-21830	CVE-2023-22040
CVE-2022-41881	CVE-2023-21949	CVE-2023-22041
CVE-2022-41915	CVE-2023-21950	CVE-2023-22042
CVE-2022-41966	CVE-2023-21961	CVE-2023-22043
CVE-2022-42003	CVE-2023-21971	CVE-2023-22044
CVE-2022-42004	CVE-2023-21974	CVE-2023-22045
CVE-2022-42890	CVE-2023-21975	CVE-2023-22046
CVE-2022-42898	CVE-2023-21983	CVE-2023-22047
CVE-2022-42920	CVE-2023-21994	CVE-2023-22048
CVE-2022-43548	CVE-2023-22004	CVE-2023-22049
CVE-2022-43680	CVE-2023-22005	CVE-2023-22050
CVE-2022-4450	CVE-2023-22006	CVE-2023-22051
CVE-2022-45047	CVE-2023-22007	CVE-2023-22052
CVE-2022-45061	CVE-2023-22008	CVE-2023-22053
CVE-2022-45143	CVE-2023-22009	CVE-2023-22054
CVE-2022-45199	CVE-2023-22010	CVE-2023-22055
CVE-2022-45688	CVE-2023-22011	CVE-2023-22056
CVE-2022-45693	CVE-2023-22012	CVE-2023-22057
CVE-2022-45787	CVE-2023-22013	CVE-2023-22058
CVE-2022-46153	CVE-2023-22014	CVE-2023-22060
CVE-2022-46364	CVE-2023-22016	CVE-2023-22061
CVE-2022-48285	CVE-2023-22017	CVE-2023-22062
CVE-2022-4899	CVE-2023-22018	CVE-2023-22809
CVE-2023-0215	CVE-2023-22020	CVE-2023-22899
CVE-2023-0286	CVE-2023-22021	CVE-2023-23914
CVE-2023-0361	CVE-2023-22022	CVE-2023-23931
CVE-2023-0464	CVE-2023-22023	CVE-2023-24998

CVE-2023-25193	CVE-2023-2650	CVE-2023-28709
CVE-2023-25194	CVE-2023-27901	CVE-2023-28856
CVE-2023-25690	CVE-2023-28439	CVE-2023-29007
CVE-2023-26049	CVE-2023-28484	CVE-2023-30535
CVE-2023-26119	CVE-2023-28708	CVE-2023-30861

Impacto

Vulnerabilidades de riesgo crítico

CVE-2022-1471: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Hospitality Cruise Shipboard Property Management System, JD Edwards EnterpriseOne Orchestrator, Siebel CRM, PeopleSoft Enterprise PeopleTools, Business Intelligence Enterprise Edition, varios en Oracle Communications Applications). CVSS: 9.8.

CVE-2021-42575: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (BI Publisher, varios en Oracle Communications Applications, y Oracle JDeveloper). CVSS: 9.8.

CVE-2022-46364: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (varios en Oracle Communications Applications Y Oracle Banking). CVSS: 9.8.

CVE-2022-31692: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (varios en Oracle Communications Applications). CVSS: 9.8.

CVE-2023-20873: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Hospitality Cruise Shipboard Property Management System, varios en Oracle Communications Applications). CVSS: 9.8.

CVE-2023-20862: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Retail Advanced Inventory Planning, varios en Oracle Communications Applications), via múltiples protocolos a MySQL Enterprise Monitor. CVSS: 9.8.

CVE-2022-37434: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Agile Engineering Data Management, Oracle AutoVue, varios en Oracle Communications Applications) y via múltiples protocolos en Oracle Hospitality Simphony. CVSS: 9.8.

CVE-2022-36944: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (varios en Oracle Communications Applications). CVSS: 9.8.

CVE-2022-23305: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (varios en Oracle Communications Applications). CVSS: 9.8.

CVE-2023-25690: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Enterprise Data Quality, varios en Oracle Communications Applications), via HTTPS en Oracle HTTP Server. CVSS: 9.8.

CVE-2022-45047: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via SSH comprometer un programa afectado (varios en Oracle Communications Applications). CVSS: 9.8.

CVE-2022-42920: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle BAM). CVSS: 9.8.

CVE-2022-41853: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Middleware Common Libraries and Tools). CVSS: 9.8.

CVE-2021-43113: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (OracleWebCenter Content). CVSS: 9.8.

CVE-2023-26119: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle WebLogic Server). CVSS: 9.8.

CVE-2022-29361: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Business Intelligence Enterprise Edition). CVSS: 9.8.

CVE-2019-17531: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Business Intelligence Enterprise Edition). CVSS: 9.8.

CVE-2019-13990: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Business Intelligence Enterprise Edition). CVSS: 9.8.

CVE-2022-33980: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Business Intelligence Enterprise Edition). CVSS: 9.8.

CVE-2021-24112: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle Hyperion Data Relationship Management). CVSS: 9.8.

CVE-2022-27404: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer un programa afectado (Oracle AutoVue). CVSS: 9.8.

CVE-2020-35169: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via XMPP comprometer Oracle Communications Billing and Revenue Management, Oracle SOA Suite, Oracle HTTP Server, Oracle Business Intelligence Enterprise, MySQL Enterprise Monitor. CVSS: 9.1.

CVE-2023-23914: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer a Oracle HTTP Server. CVSS: 9.1.

CVE-2021-23926: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer a Oracle SOA Suite. CVSS: 9.1.

CVE-2018-1282: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer a Oracle Business Intelligence Enterprise Edition. Suite. CVSS: 9.1.

CVE-2022-37865: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via múltiples protocolos comprometer a MySQL Enterprise Monitor. CVSS: 9.1.

CVE-2023-21974: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer a Application Express Team Calendar Plugin. Suite. CVSS: 9.0.

CVE-2023-21975: Vulnerabilidad de fácil explotación, permite a un atacante no autenticado con acceso de red via HTTP comprometer a Application Express Customers Plugin. Suite. CVSS: 9.0.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Oracle Communications Billing and Revenue Management 12.0.0.4.0-12.0.0.8.0
Oracle Communications Convergence 3.0.3.2
Oracle Communications Messaging Server 8.1.0.21.0
Oracle Communications Unified Assurance 5.5.0-5.5.17, 6.0.0-6.0.2
Oracle Communications Unified Inventory Management 7.4.1, 7.4.2
Oracle Communications Diameter Signaling Router 8.6.0.0
Oracle Communications Network Analytics Data Director 23.1.0
Oracle Application Testing Suite 13.3.0.1

Oracle Enterprise Manager Ops Center 12.4.0.0
Oracle Banking Corporate Lending 14.0-14.3, 14.5-14.7
Oracle BAM (Business Activity Monitoring) 12.2.1.4.0
Oracle Middleware Common Libraries and Tools 12.2.1.4.0
Oracle WebCenter Content 12.2.1.4.0
Oracle WebLogic Server 12.2.1.4.0, 14.1.1.0.0
Oracle Business Intelligence Enterprise Edition 6.4.0.0.0
Oracle Business Intelligence Enterprise Edition 12.2.1.4.0
Oracle Hyperion Data Relationship Management 11.2.13.0.000
Oracle AutoVue 21.0.2.0-21.0.2.7
Oracle Communications Billing and Revenue Management 12.0.0.4.0-12.0.0.7.0
Oracle HTTP Server 12.2.1.4.0
Oracle SOA Suite 12.2.1.4.0
Oracle Business Intelligence Enterprise Edition 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0
MySQL Enterprise Monitor 8.0.34 and prior
Application Express Customers Plugin Application Express Customers Plugin: 18.2-22.2
Application Express Team Calendar Plugin Application Express Team Calendar Plugin: 18.2-22.1
Oracle Communications BRM - Elastic Charging Engine 12.0.0.4.0-12.0.0.8.0
Oracle Communications Cloud Native Core Binding Support Function 22.4.0, 23.1.0
Oracle Banking APIs 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
BI Publisher 7.0.0.0.0
Oracle Hyperion Financial Reporting 11.2.13.0.000
PeopleSoft Enterprise PeopleTools 8.59, 8.60
Oracle Business Intelligence Enterprise Edition 6.4.0.0.0, 7.0.0.0.0
Oracle TimesTen In-Memory Database 22.1.1.1.0-22.1.1.6.0
JD Edwards EnterpriseOne Tools Prior to 9.2.7.3
Oracle VM VirtualBox Prior to 6.1.46, Prior to 7.0.10
Oracle Enterprise Data Quality 12.2.1.4.0
Oracle Solaris 11
Oracle Hyperion Workspace 11.2.13.0.000
Oracle Graph Server and Client 21.4.6, 22.4.2, 23.1.0
Oracle Commerce Guided Search 11.3.2
Oracle Commerce Platform 11.3.0, 11.3.1, 11.3.2
Oracle Communications BRM - Elastic Charging Engine 12.0.0.4.0-12.0.0.6.0
Oracle Communications Instant Messaging Server 10.0.1.7.0
Oracle Communications Unified Inventory Management 7.4.0-7.4.2, 7.5.0
Oracle Communications Cloud Native Core Automated Test Suite 23.1.1
Oracle Communications Cloud Native Core Automated Test Suite 22.4.1, 23.1.0
Oracle Communications Cloud Native Core Network Exposure Function 22.4.3, 23.1.2
Oracle Communications Cloud Native Core Network Function Cloud Native Environment 23.1.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy 23.1.2, 22.4.3
Oracle Communications Cloud Native Core Service Communication Proxy 22.4.0, 23.1.0
Oracle Communications Cloud Native Core Unified Data Repository 23.1.1
Oracle Banking Branch 14.5-14.7

Oracle Banking Cash Management 14.7.0.2.0, 14.7.1.0.0
Oracle Banking Trade Finance 14.0-14.3, 14.5-14.7
Oracle Access Manager 12.2.1.4.0
Oracle Identity Manager 12.2.1.4.0
Oracle Service Bus 12.2.1.4.0
MySQL Cluster 8.0.33 and prior
Siebel CRM 23.4 and prior
Siebel CRM 23.6 and prior
Siebel CRM 22.12 and prior
Primavera Gateway 18.8.0-18.8.15, 19.12.0-19.12.16, 20.12.0-20.12.11, 21.12.0-21.12.9
Oracle Communications Network Integrity 7.3.6.4
Oracle Communications Order and Service Management 7.4.1
Oracle Communications Pricing Design Center 12.0.0.4.0-12.0.0.7.0
Oracle Communications Cloud Native Core Network Repository Function 23.1.0, 23.2.0
Oracle Communications Cloud Native Core Network Repository Function 23.1.1
Oracle Web Applications Desktop Integrator 12.2.3-12.2.12
Oracle Enterprise Manager for Fusion Middleware 13.5.0.0
Oracle Enterprise Manager for Oracle Database 13.5.0.0
Oracle Data Integrator 12.2.1.4.0
Oracle Mobile Security Suite Prior to 11.1.2.3.1
Oracle Health Sciences Sciences Data Management Workbench 3.1.0.2, 3.1.1.3, 3.2.0.0
Oracle GoldenGate Stream Analytics 19.1.0.0.0-19.1.0.0.7
Oracle Applications Framework 12.2.3-12.3.12
Oracle Scripting 12.2.3-12.2.12
BI Publisher 6.4.0.0.0
JD Edwards EnterpriseOne Tools Prior to 9.2.7.4
Siebel CRM 23.5 and prior
Oracle Hyperion Essbase Administration Services 21.4.3.0.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy 23.1.2
Oracle Java SE Oracle Java SE: 8u371
MySQL Server 5.7.42 and prior, 8.0.33 and prior
Application Express Administration Application Express Administration: 18.2-22.2
Oracle Communications Cloud Native Core Console 22.4.2, 23.1.1
Oracle Business Process Management Suite 12.2.1.4.0
Oracle WebLogic Server 14.1.1.0.0
JD Edwards EnterpriseOne Orchestrator Prior to 9.2.7.4
Oracle Agile PLM 9.3.6
Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1
Unified Audit 19.3-19.19, 21.3-21.10
MySQL Server 8.0.33 and prior
MySQL Server 8.0.27 and prior
MySQL Server 5.7.41 and prior, 8.0.32 and prior

Oracle WebLogic Server 14.1.1.0.0, 12.2.1.4.0
Oracle Applications Technology 12.2.3-12.2.12
Oracle Self-Service Human Resources 12.2.3-12.2.12
Oracle Business Intelligence Enterprise Edition 7.0.0.0.0
Advanced Networking Option 19.3-19.19, 21.3-21.10
Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1
Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1
Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1
Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1
Java VM 19.3-19.19, 21.3-21.10
Oracle Essbase 21.4.3.0.0

Enlaces

https://www.oracle.com/security-alerts/cpujul2023.html
https://www.oracle.com/security-alerts/cpujul2023verbose.html#CAGBU
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1282
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0227
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10086
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10735
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13936
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13956
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35168
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35169
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-36518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7760
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8908
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22569
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24112
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-25220
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26117
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28168

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36090
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-36374
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40690
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41183
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42575
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43113
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-46877
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1122
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1471
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22971
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-2022-23491
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24409
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24891
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25147
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27404
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29361
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29546
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-2963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31129
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31160
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-31197
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-2022-31777
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33879
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-33980
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36944
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37434
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-37865

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40150
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40152
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40897
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41853
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41881
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41915
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41966
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42003
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42898
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42920
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-2022-4450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45143
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45199
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45688
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45693
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-45787
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-46153
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-46364
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-48285
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-4899
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0215
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0286
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0361
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0464
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0767
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1370
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1436
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-1999
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20860
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20861
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20862
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20863
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20873
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21830
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21949
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21950
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21961
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21971

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21974
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21975
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21983
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-21994
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22004
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22005
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22006
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22008
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22009
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22010
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22011
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22012
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22013
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22014
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22016
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22017
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22018
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22020
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22027
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22031
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22033
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22034
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22035
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22036
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22037
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22042
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22045
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22046
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22047
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22048
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22050
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22051
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22052

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22053
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22054
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22055
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22056
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22057
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22058
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22060
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22061
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22062
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22809
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-22899
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23914
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-23931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-24998
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25193
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25194
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25690
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26049
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-26119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2650
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27901
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28484
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28709
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28856
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-29007
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30535
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30861

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.24 18:48:24 -04'00'