Alerta de seguridad cibernética	9VSA22-00678-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	21 de julio de 2022
Última revisión	21 de julio de 2022

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 Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre nuevas vulnerabilidades dadas a conocer por Oracle, como parte de su reporte Critical Patch Update (CPU) trimestral de julio.

Vulnerabilidades

CVE-2018-1273
CVE-2018-25032
CVE-2019-0219
CVE-2019-0220
CVE-2019-0227
CVE-2019-10082
CVE-2019-10086
CVE-2019-17495
CVE-2019-20916
CVE-2020-10683
CVE-2020-11022
CVE-2020-11023
CVE-2020-11987
CVE-2020-14343
CVE-2020-17521
CVE-2020-1927
CVE-2020-25649
CVE-2020-26237
CVE-2020-28052
CVE-2020-28491
CVE-2020-35169
CVE-2020-36518
CVE-2020-5258
CVE-2020-7656
CVE-2020-7712
CVE-2020-9492
CVE-2021-22118
CVE-2021-22119
CVE-2021-22931
CVE-2021-22946
CVE-2021-23337
CVE-2021-23450
CVE-2021-2351
CVE-2021-23926
CVE-2021-26291
CVE-2021-29425
CVE-2021-29505
CVE-2021-30129
CVE-2021-31684
CVE-2021-3177
CVE-2021-31805
CVE-2021-31812
CVE-2021-33813
CVE-2021-34141
CVE-2021-34429
CVE-2021-3450
CVE-2021-3572
CVE-2021-35940
CVE-2021-36090
CVE-2021-36374
CVE-2021-37137
CVE-2021-3749
CVE-2021-37714
CVE-2021-37750
CVE-2021-38153
CVE-2021-38296
CVE-2021-39139
CVE-2021-40690
CVE-2021-41182
CVE-2021-41184
CVE-2021-41303
CVE-2021-42340
CVE-2021-42575
CVE-2021-43797
CVE-2021-43859
CVE-2021-44832
CVE-2021-45943
CVE-2022-0778
CVE-2022-0839
CVE-2022-1154
CVE-2022-1271
CVE-2022-1292
CVE-2022-21428
CVE-2022-21429
CVE-2022-21432
CVE-2022-21439
CVE-2022-21455
CVE-2022-21500
CVE-2022-21508
CVE-2022-21509
CVE-2022-21510
CVE-2022-21511
CVE-2022-21512
CVE-2022-21513

CVE-2022-21514	CVE-2022-21540	CVE-2022-21567	CVE-2022-22969
CVE-2022-21515	CVE-2022-21541	CVE-2022-21568	CVE-2022-22971
CVE-2022-21516	CVE-2022-21542	CVE-2022-21569	CVE-2022-22978
CVE-2022-21517	CVE-2022-21543	CVE-2022-21570	CVE-2022-23181
CVE-2022-21518	CVE-2022-21544	CVE-2022-21571	CVE-2022-23219
CVE-2022-21519	CVE-2022-21545	CVE-2022-21572	CVE-2022-23305
CVE-2022-21520	CVE-2022-21547	CVE-2022-21573	CVE-2022-23308
CVE-2022-21521	CVE-2022-21548	CVE-2022-21574	CVE-2022-23437
CVE-2022-21522	CVE-2022-21549	CVE-2022-21575	CVE-2022-23457
CVE-2022-21523	CVE-2022-21550	CVE-2022-21576	CVE-2022-23632
CVE-2022-21524	CVE-2022-21551	CVE-2022-21577	CVE-2022-24329
CVE-2022-21525	CVE-2022-21552	CVE-2022-21578	CVE-2022-24407
CVE-2022-21526	CVE-2022-21553	CVE-2022-21579	CVE-2022-24729
CVE-2022-21527	CVE-2022-21554	CVE-2022-21580	CVE-2022-24735
CVE-2022-21528	CVE-2022-21555	CVE-2022-21581	CVE-2022-24801
CVE-2022-21529	CVE-2022-21556	CVE-2022-21582	CVE-2022-24823
CVE-2022-21530	CVE-2022-21557	CVE-2022-21583	CVE-2022-24839
CVE-2022-21531	CVE-2022-21558	CVE-2022-21584	CVE-2022-25636
CVE-2022-21532	CVE-2022-21559	CVE-2022-21585	CVE-2022-25647
CVE-2022-21533	CVE-2022-21560	CVE-2022-21586	CVE-2022-25762
CVE-2022-21534	CVE-2022-21561	CVE-2022-21824	CVE-2022-25845
CVE-2022-21535	CVE-2022-21562	CVE-2022-22721	CVE-2022-27778
CVE-2022-21536	CVE-2022-21563	CVE-2022-22947	CVE-2022-29577
CVE-2022-21537	CVE-2022-21564	CVE-2022-22963	CVE-2022-29885
CVE-2022-21538	CVE-2022-21565	CVE-2022-22965	CVE-2022-30126
CVE-2022-21539	CVE-2022-21566	CVE-2022-22968	CVE-2022-34169

Impacto

Vulnerabilidades de mayor riesgo crítico

CVE-2022-22947: Vulnerabilidad fácil de explotar en varios productos de Oracle Communications (BSF, CNC Console, NRF y SEPP de Spring Cloud Gateway). Permite su compromiso por un atacante no autenticado con acceso de red a través de HTTP. Puntaje CVSS 10.

Productos afectados

Big Data Spatial and Graph anterior a 23.1
Enterprise Manager Base Platform 13.4.0.0, 13.5.0.0
Enterprise Manager Ops Center 12.4.0.0
Java VM 12.1.0.2, 19c, 21c
JD Edwards EnterpriseOne Orchestrator 9.2.6.3 y anterior
JD Edwards EnterpriseOne Tools 9.2.6.1 y anterior
JD Edwards EnterpriseOne Tools 9.2.6.3 y anterior
MySQL Cluster 8.0.29 y anterior
MySQL Cluster 7.4.36 y anterior,7.5.26 y anterior, 7.6.22 y anterior, y 8.0.29 y anterior
MySQL Enterprise Monitor 8.0.30 y anterior

MySQL Enterprise Monitor 8.0.25 y anterior
MySQL Enterprise Monitor 8.0.29 y anterior
MySQL Server 5.7.38 y anterior, 8.0.29 y anterior
MySQL Server 8.0.28 y anterior
MySQL Server 8.0.29 y anterior
MySQL Shell 8.0.28 y anterior
MySQL Shell for VS Code 1.1.8 y anterior
MySQL Workbench 8.0.29 y anterior
Oracle Agile Engineering Data Management 6.2.1.0
Oracle Agile PLM 9.3.6
Oracle Agile Product Lifecycle Management for Process 6.2.2, 6.2.3
Oracle Application Express (CKEditor) anterior a 22.1.1
Oracle Application Express (jQueryUI) anterior a 22.1.1
Oracle Application Testing Suite 13.3.0.1
Oracle Applications Framework 12.2.9-12.2.11
Oracle Autovue for Agile Product Lifecycle Management 21.0.2
Oracle Banking Branch 14.5
Oracle Banking Cash Management 14.5
Oracle Banking Corporate Lending Process Management 14.5
Oracle Banking Credit Facilities Process Management 14.5
Oracle Banking Deposits and Lines of Credit Servicing 2.7
Oracle Banking Electronic Data Exchange for Corporates 14.5
Oracle Banking Liquidity Management 14.2, 14.5
Oracle Banking Origination 14.5
Oracle Banking Party Management 2.7
Oracle Banking Platform 2.6.2
Oracle Banking Platform 2.9, 2.12
Oracle Banking Supply Chain Finance 14.5
Oracle Banking Trade Finance 14.5
Oracle Banking Trade Finance Process Management 14.5
Oracle Banking Virtual Account Management 14.5
Oracle BI Publisher 12.2.1.3.0, 12.2.1.4.0
Oracle Business Intelligence Enterprise Edition 5.9.0.0.0
Oracle Coherence 14.1.1.0.0
Oracle Coherence 3.7.1.0, 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
Oracle Commerce Guided Search 11.3.2
Oracle Commerce Merchandising 11.3.2
Oracle Commerce Platform 11.3.2
Oracle Commerce Platform 11.3.0, 11.3.1, 11.3.2
Oracle Communications ASAP 7.3
Oracle Communications Billing and Revenue Management 12.0.0.4.0-12.0.0.6.0
Oracle Communications BRM - Elastic Charging Engine anterior a 12.0.0.4.6, anterior a 12.0.0.5.1
Oracle Communications Cloud Native Core Binding Support Function 22.1.3
Oracle Communications Cloud Native Core Binding Support Function 22.2.0
Oracle Communications Cloud Native Core Console 22.2.0

Oracle Communications Cloud Native Core Console 22.1.2
Oracle Communications Cloud Native Core Network Exposure Function 22.1.1
Oracle Communications Cloud Native Core Network Function Cloud Native Environment 22.1.0
Oracle Communications Cloud Native Core Network Function Cloud Native Environment 22.2.0
Oracle Communications Cloud Native Core Network Function Cloud Native Environment 22.1.2
Oracle Communications Cloud Native Core Network Repository Function 22.1.2, 22.2.0
Oracle Communications Cloud Native Core Network Slice Selection Function 22.1.1
Oracle Communications Cloud Native Core Policy 22.1.3
Oracle Communications Cloud Native Core Policy 22.2.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy 22.1.1
Oracle Communications Cloud Native Core Service Communication Proxy 22.2.0
Oracle Communications Cloud Native Core Unified Data Repository 22.2.0
Oracle Communications Core Session Manager 8.2.5, 8.4.5
Oracle Communications Design Studio 7.4.2
Oracle Communications Instant Messaging Server 10.0.1.5.0
Oracle Communications Offline Mediation Controller anterior a 12.0.0.4.4, anterior a 12.0.0.5.1
Oracle Communications Operations Monitor 4.3, 4.4, 5.0
Oracle Communications Session Border Controller 8.4, 9.0, 9.1
Oracle Communications Unified Inventory Management 7.5.0
Oracle Communications Unified Inventory Management 7.4.1, 7.4.2, 7.5.0
Oracle Communications Unified Session Manager 8.2.5
Oracle Crystal Ball 11.1.2.0.000-11.1.2.4.900
Oracle Database - Enterprise Edition 12.1.0.2, 19c, 21c
Oracle Database - Enterprise Edition RDBMS Security 12.1.0.2, 19c, 21c
Oracle Database - Enterprise Edition Recovery None
Oracle Database - Enterprise Edition Sharding None
Oracle E-Business Suite Information Discovery 12.2.3-12.2.11
Oracle Enterprise Communications Broker 3.3
Oracle Enterprise Operations Monitor 4.3, 4.4, 5.0
Oracle Enterprise Session Border Controller 8.4, 9.0, 9.1
Oracle Essbase 21.3
Oracle Financial Services Analytical Applications Infrastructure 8.0.7.0-8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1
Oracle Financial Services Behavior Detection Platform 8.0.7.0, 8.0.8.0, 8.1.1.0-8.1.2.1
Oracle Financial Services Crime and Compliance Management Studio 8.0.8.2.0, 8.0.8.3.0
Oracle Financial Services Enterprise Case Management 8.0.7.1, 8.0.7.2, 8.0.8.0, 8.0.8.1, 8.1.1.0-8.1.2.1
Oracle Financial Services Revenue Management and Billing 2.9.0.0.0, 2.9.0.1.0, 3.0.0.0.0-3.2.0.0.0, 4.0.0.0.0
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition 8.0.7.0, 8.0.8.0
Oracle FLEXCUBE Core Banking 5.2, 11.6-11.8, 11.10
Oracle FLEXCUBE Private Banking 12.1
Oracle FLEXCUBE Universal Banking 12.1-12.4, 14.0-14.3, 14.5
Oracle FLEXCUBE Universal Banking 12.4
Oracle FLEXCUBE Universal Banking 12.3, 12.4, 14.0-14.3, 14.5
Oracle Global Lifecycle Management NextGen OUI Framework anterior a 13.9.4.2.10

Oracle Global Lifecycle Management OPatch anterior a 12.2.0.1.30
Oracle GoldenGate 21c: anterior a 21.7.0.0.0
Oracle GoldenGate 21c: anterior a 21.7.0.0.0; 19c: anterior a 19.1.0.0.220719
Oracle GraalVM Enterprise Edition Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2, 22.1.0
Oracle Graph Server and Client anterior a 22.2.0
Oracle Health Sciences Data Management Workbench 2.5.2.1, 3.0.0.0
Oracle Health Sciences Data Management Workbench 2.5.2.1, 3.0.0.0, 3.1.0.3
Oracle Health Sciences Data Management Workbench 2.4.8.7, 2.5.2.1
Oracle Health Sciences Empirica Signal 9.1.0.52, 9.2.0.52
Oracle Health Sciences Information Manager 3.0.0.1, 3.0.1.0-3.0.5.0
Oracle Healthcare Foundation 8.1.0, 8.2.0, 8.2.1
Oracle Hospitality Cruise Shipboard Property Management System 20.2.1
Oracle Hospitality Inventory Management 9.1
Oracle Hospitality Materials Control 18.1
Oracle Hospitality OPERA 5 5.6
Oracle HTTP Server 12.2.1.3.0, 12.2.1.4.0
Oracle HTTP Server 12.2.1.3.0
Oracle iReceivables 12.2.3-12.2.11
Oracle iRecruitment 12.2.3-12.2.11
Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2, 22.1.0
Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle Java SE: 17.0.3.1; Oracle GraalVM Enterprise Edition: 21.3.2, 22.1.0
Oracle Managed File Transfer 12.2.1.3.0, 12.2.1.4.0
Oracle Middleware Common Libraries and Tools 12.2.1.3.0, 12.2.1.4.0
Oracle Policy Automation 12.2.0-12.2.24
Oracle Policy Automation 12.2.0-12.2.25
Oracle Policy Automation for Mobile Devices 12.2.0-12.2.24
Oracle Product Lifecycle Analytics 3.6.1
Oracle REST Data Services anterior a 22.1.1
Oracle Retail Allocation 15.0.3.1, 16.0.3
Oracle Retail Bulk Data Integration 16.0.3
Oracle Retail Customer Insights 15.0.2, 16.0.2
Oracle Retail Customer Insights 16.0.2
Oracle Retail Customer Management and Segmentation Foundation 17.0, 18.0, 19.0
Oracle Retail Extract Transform and Load 13.2.5
Oracle Retail Financial Integration 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
Oracle Retail Integration Bus 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1
Oracle Retail Merchandising System 16.0.3, 19.0.1
Oracle Retail Order Broker 18.0, 19.1
Oracle Retail Pricing 19.0.1
Oracle Retail Sales Audit 15.0.3.1
Oracle Retail Sales Audit 16.0.3
Oracle Retail Xstore Point of Service 17.0.4, 18.0.3, 19.0.2, 20.0.1, 21.0.1
Oracle Retail Xstore Point of Service 17.0.4, 18.0.3, 19.0.2, 20.0.1

Oracle SD-WAN Edge 9.0, 9.1
Oracle Security Service 12.2.1.3.0, 12.2.1.4.0
Oracle SOA Suite 12.2.1.3.0, 12.2.1.4.0
Oracle Solaris 11
Oracle Solaris 10, 11
Oracle Spatial and Graph (GDAL) 19c, 21c
Oracle Spatial Studio anterior a 22.1.0
Oracle SQLcl (Liquibase) 19c
Oracle Stream Analytics 19c: anterior a 19.1.0.0.6.4
Oracle TimesTen In-Memory Database anterior a 22.1.1.1.0
Oracle Transportation Management 1.4.4
Oracle User Management 12.2.4-12.2.11
Oracle Utilities Framework 4.3.0.5.0, 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 VM VirtualBox anterior a 6.1.36
Oracle WebCenter Content 12.2.1.3.0, 12.2.1.4.0
Oracle WebCenter Portal 12.2.1.3.0, 12.2.1.4.0
Oracle WebCenter Sites Support Tools anterior a 4.4.2
Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
Oracle WebLogic Server 12.2.1.4.0, 14.1.1.0.0
Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0
Oracle Weblogic Server Proxy Plug-in 12.2.1.3.0, 12.2.1.4.0
Oracle Workflow 12.2.3-12.2.11
Oracle ZFS Storage Appliance Kit 8.8
PeopleSoft Enterprise PeopleTools 8.58, 8.59
PeopleSoft Enterprise PeopleTools 8.58
Primavera Gateway 17.12.0-17.12.11, 18.8.0-18.8.14, 19.12.0-19.12.13, 20.12.0-20.12.8, 21.12.0-21.12.1
Primavera Gateway 17.12.0-17.12.11, 18.8.0-18.8.14, 19.12.0-19.12.13, 20.12.0-20.12.8
Primavera P6 Enterprise Project Portfolio Management 17.12.0.0-17.12.20.4, 18.8.0.0-18.8.25.4, 19.12.0.0-19.12.19.0, 20.12.0.0-20.12.14.0, 21.12.0.0-21.12.4.0
Primavera Unifier 17.7-17.12, 18.8, 19.12, 20.12, 21.12
Product Supported Versions Affected
Siebel Apps - Field Service 22.6 y anterior

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.oracle.com/security-alerts/cpujul2022.html
https://www.oracle.com/security-alerts/cpujul2022verbose.html#DB
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-2019-0219
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0220
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0227

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10082
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10086
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17495
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20916
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-10683
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14343
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1927
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-25649
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26237
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28052
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28491
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-2020-5258
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7656
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7712
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9492
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22118
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22931
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23337
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-2351
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-23926
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26291
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29505
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30129
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-31684
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3177
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-2021-33813
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34141
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3450
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3572
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35940
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-2021-37137
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3749
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37714
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37750
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38153
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-38296
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-39139
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40690
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41184
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-41303
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42340
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-42575
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43797
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-43859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45943
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0839
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1154
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1292
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21428
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21432
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21439
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21455
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21500
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21508
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21509
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21510
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21511
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21512
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21513
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21514
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21515
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21516
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21517
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21518
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21519
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21520
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21521
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21522
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21523
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21524

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21525
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21526
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21527
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21528
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21529
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21530
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21531
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21532
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21533
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21534
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21535
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21536
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21537
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21538
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21539
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21540
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21541
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21542
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21543
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21544
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21545
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21547
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21548
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21549
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21550
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21551
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21552
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21553
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21554
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21555
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21556
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21557
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21558
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21559
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21560
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21561
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21562
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21563
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21564
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21565
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21566
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21567
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21568
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21569
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21570

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21571
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21572
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21573
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21574
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21575
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21576
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21577
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21578
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21579
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21580
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21581
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21582
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21583
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21584
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21585
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21586
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21824
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22721
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22947
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22965
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22968
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22969
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-2022-23181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23305
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23308
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-2022-23632
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-2022-24729
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24735
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-24801
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-2022-25636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25647
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25762
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25845
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27778
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29577

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29885
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30126
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34169