Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

22-07-2022 | Año 4 | N°159

Boletín de Seguridad Cibernética

Semana del 15 al 21 de julio de 2022

La semana en cifras

Parches

237

para vulnerabilidades

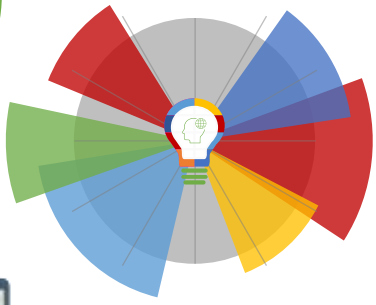
Las mitigaciones son útiles en productos de Oracle, Cisco y Google.

Hash

2

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

20

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

4

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

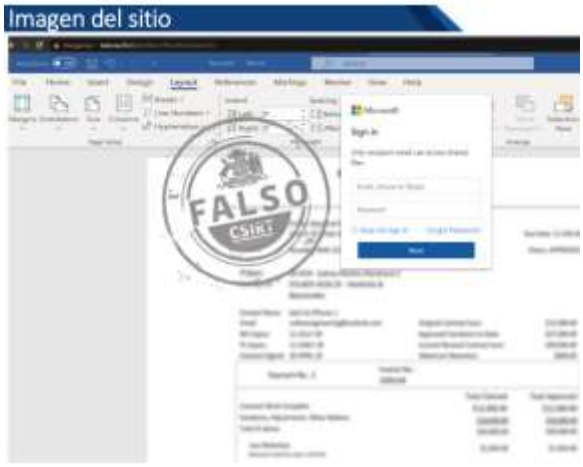
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Malware

CSIRT alerta ante campaña de phishing que suplanta a DHL	
Alerta de seguridad cibernética	2CMV21-00307-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Julio de 2021
Última revisión	19 de Julio de 2021
Indicadores de compromiso	
SHA256	
Nombre: DHL_119040 de recibo,pdf.img SHA256: a3ba3f9f24cb4588b5f5943e1f06b96ca25d425424e804c30074e624c164d14e	
Nombre: DHL_119040 de recibo,pdf.exe	
Nombre: HGHJJKYUHJJJDSD456.exe SHA256: 6576ca8629f0a914f2689637d670f0b1fc58b3bd0d9d3a04d3a32e716496dee8	
IoC URL	
mail.tycautomotriz[.]cl https://secure.comodo[.]com/CPS0L http://ocsp.sectigo[.]com/ http://ocsp.comodoca[.]com/ http://ocsp.usertrust[.]com/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00307-01/	
https://www.csirt.gob.cl/media/2022/07/2CMV22-00307-PH-01.pdf	

Sitios fraudulentos



CSIRT alerta de página fraudulenta que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR22-01091-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de julio de 2022
Última revisión	15 de julio de 2022
Indicadores de compromiso	
URL sitio falso	
https://baterias20[.]cl/p0o9i8u/Office365/index.html	
IP	
[200.63.99.34]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01091-01/	
https://www.csirt.gob.cl/media/2022/06/8FFR22-01091-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00560-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de julio de 2022
Última revisión	15 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3Pt4Qmq?l=www.bancoripley.cl http://ruslang[.]today/activacion/cuenta-djik/	
URL sitio falso	
https://bancoripley.cl.muraridasbabaji[.]org/1657891945/login	
IP	
[96.127.183.234]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00560-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00560-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00561-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2022
Última revisión	18 de julio de 2022
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3AVOU8e https://mexican.softcorp[.]ca/49	
URL sitio falso	
https://officebanqing[.]space/	
IP	
[54.90.99.6]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00561-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00561-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00562-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2022
Última revisión	18 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://contribvalpa[.]com/promocion/cuenta-jhrg/	
URL sitio falso	
https://www.theoutboxsolutions[.]com/nhjyg/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[173.201.177.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00562-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00562-01.pdf	

CSIRT alerta de phishing con falso cambio de clave Santander	
Alerta de seguridad cibernética	8FPH22-00563-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de julio de 2022
Última revisión	19 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3RNsbBh?l=www.santander.cl https://gurujam[.]com/activacion/cuenta-jqrl/	
URL sitio falso	
http://banco.santander.cl.armeniantube[.]net/1658250041/portada/personas/home.asp	
IP	
[69.49.231.247]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00563-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00563-01.pdf	

CSIRT advierte phishing que suplanta al correo Zimbra	
Alerta de seguridad cibernética	8FPH22-00564-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de julio de 2022
Última revisión	20 de julio de 2022
Indicadores de compromiso	
URL Redirección	
https://trzimbrawebadd.weebly[.]com/	
IP	
[199.34.228.54]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00564-01/	
https://www.csirt.gob.cl/media/2022/07/8FPH22-00564-01.pdf	

Vulnerabilidades

CSIRT alerta de nuevas vulnerabilidades en Chrome OS	
Alerta de seguridad cibernética	9VSA22-00677-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de julio de 2022
Última revisión	18 de julio de 2022
CVE	
CVE-2022-2156 CVE-2022-2294 CVE-2021-30560 CVE-2022-29824	
Fabricantes	
SAP	
Productos afectados	
Chrome OS anterior a 102.0.5005.153	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00677-01/	
https://www.csirt.gob.cl/media/2022/07/9VSA22-00677-01.pdf	

CSIRT comparte vulnerabilidades entregadas por Oracle (CPU julio 2022)		
Alerta de seguridad cibernética	9VSA22-00678-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	21 de julio de 2022	
Última revisión	21 de julio de 2022	
CVE		
CVE-2018-1273	CVE-2021-43797	CVE-2022-21557
CVE-2018-25032	CVE-2021-43859	CVE-2022-21558
CVE-2019-0219	CVE-2021-44832	CVE-2022-21559
CVE-2019-0220	CVE-2021-45943	CVE-2022-21560
CVE-2019-0227	CVE-2022-0778	CVE-2022-21561
CVE-2019-10082	CVE-2022-0839	CVE-2022-21562
CVE-2019-10086	CVE-2022-1154	CVE-2022-21563
CVE-2019-17495	CVE-2022-1271	CVE-2022-21564
CVE-2019-20916	CVE-2022-1292	CVE-2022-21565
CVE-2020-10683	CVE-2022-21428	CVE-2022-21566
CVE-2020-11022	CVE-2022-21429	CVE-2022-21567
CVE-2020-11023	CVE-2022-21432	CVE-2022-21568
CVE-2020-11987	CVE-2022-21439	CVE-2022-21569
CVE-2020-14343	CVE-2022-21455	CVE-2022-21570
CVE-2020-17521	CVE-2022-21500	CVE-2022-21571

CVE-2020-1927	CVE-2022-21508	CVE-2022-21572
CVE-2020-25649	CVE-2022-21509	CVE-2022-21573
CVE-2020-26237	CVE-2022-21510	CVE-2022-21574
CVE-2020-28052	CVE-2022-21511	CVE-2022-21575
CVE-2020-28491	CVE-2022-21512	CVE-2022-21576
CVE-2020-35169	CVE-2022-21513	CVE-2022-21577
CVE-2020-36518	CVE-2022-21514	CVE-2022-21578
CVE-2020-5258	CVE-2022-21515	CVE-2022-21579
CVE-2020-7656	CVE-2022-21516	CVE-2022-21580
CVE-2020-7712	CVE-2022-21517	CVE-2022-21581
CVE-2020-9492	CVE-2022-21518	CVE-2022-21582
CVE-2021-22118	CVE-2022-21519	CVE-2022-21583
CVE-2021-22119	CVE-2022-21520	CVE-2022-21584
CVE-2021-22931	CVE-2022-21521	CVE-2022-21585
CVE-2021-22946	CVE-2022-21522	CVE-2022-21586
CVE-2021-23337	CVE-2022-21523	CVE-2022-21824
CVE-2021-23450	CVE-2022-21524	CVE-2022-22721
CVE-2021-2351	CVE-2022-21525	CVE-2022-22947
CVE-2021-23926	CVE-2022-21526	CVE-2022-22963
CVE-2021-26291	CVE-2022-21527	CVE-2022-22965
CVE-2021-29425	CVE-2022-21528	CVE-2022-22968
CVE-2021-29505	CVE-2022-21529	CVE-2022-22969
CVE-2021-30129	CVE-2022-21530	CVE-2022-22971
CVE-2021-31684	CVE-2022-21531	CVE-2022-22978
CVE-2021-3177	CVE-2022-21532	CVE-2022-23181
CVE-2021-31805	CVE-2022-21533	CVE-2022-23219
CVE-2021-31812	CVE-2022-21534	CVE-2022-23305
CVE-2021-33813	CVE-2022-21535	CVE-2022-23308
CVE-2021-34141	CVE-2022-21536	CVE-2022-23437
CVE-2021-34429	CVE-2022-21537	CVE-2022-23457
CVE-2021-3450	CVE-2022-21538	CVE-2022-23632
CVE-2021-3572	CVE-2022-21539	CVE-2022-24329
CVE-2021-35940	CVE-2022-21540	CVE-2022-24407
CVE-2021-36090	CVE-2022-21541	CVE-2022-24729
CVE-2021-36374	CVE-2022-21542	CVE-2022-24735
CVE-2021-37137	CVE-2022-21543	CVE-2022-24801
CVE-2021-3749	CVE-2022-21544	CVE-2022-24823
CVE-2021-37714	CVE-2022-21545	CVE-2022-24839
CVE-2021-37750	CVE-2022-21547	CVE-2022-25636
CVE-2021-38153	CVE-2022-21548	CVE-2022-25647
CVE-2021-38296	CVE-2022-21549	CVE-2022-25762
CVE-2021-39139	CVE-2022-21550	CVE-2022-25845
CVE-2021-40690	CVE-2022-21551	CVE-2022-27778
CVE-2021-41182	CVE-2022-21552	CVE-2022-29577
CVE-2021-41184	CVE-2022-21553	CVE-2022-29885
CVE-2021-41303	CVE-2022-21554	CVE-2022-30126
CVE-2021-42340	CVE-2022-21555	CVE-2022-34169
CVE-2021-42575	CVE-2022-21556	
Fabricante		

Oracle
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 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

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 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
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00678-01/
https://www.csirt.gob.cl/media/2022/07/9VSA22-00678-01.pdf

CSIRT alerta de nuevas vulnerabilidades en productos Cisco	
Alerta de seguridad cibernética	9VSA22-00679-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de julio de 2022
Última revisión	21 de julio de 2022

CVE		
CVE-2022-20857	CVE-2022-20885	CVE-2022-20900
CVE-2022-20858	CVE-2022-20886	CVE-2022-20901
CVE-2022-20861	CVE-2022-20887	CVE-2022-20902
CVE-2022-20860	CVE-2022-20888	CVE-2022-20903
CVE-2022-20873	CVE-2022-20889	CVE-2022-20904
CVE-2022-20874	CVE-2022-20890	CVE-2022-20910
CVE-2022-20875	CVE-2022-20891	CVE-2022-20911
CVE-2022-20876	CVE-2022-20892	CVE-2022-20912
CVE-2022-20877	CVE-2022-20893	CVE-2022-20906
CVE-2022-20878	CVE-2022-20894	CVE-2022-20907
CVE-2022-20879	CVE-2022-20895	CVE-2022-20908
CVE-2022-20880	CVE-2022-20896	CVE-2022-20909
CVE-2022-20881	CVE-2022-20897	CVE-2022-20913
CVE-2022-20882	CVE-2022-20898	CVE-2022-20916
CVE-2022-20883	CVE-2022-20899	CVE-2022-20733
CVE-2022-20884		

Fabricante
Cisco
Productos afectados
Cisco Nexus Dashboard Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers Cisco IoT Control Center
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00679-01/
https://www.csirt.gob.cl/media/2022/07/9VSA22-00679-01.pdf

Actualidad

Ciberconsejos | Cuidados en el uso de internet por niños, niñas y adolescentes

Como los menores de edad son uno de los grupos más expuestos a engaños y contenido inapropiado en la red, decidimos recordar algunos de los principales consejos para tener en cuenta datos. Revísalos aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-nna/.

Ciberdiccionario Volumen 11

En esta nueva edición del ciberdiccionario del CSIRT de Gobierno hablamos sobre el ciberbullying, sistema operativo y explicamos la diferencia entre software y hardware. Puedes descargar estas definiciones en formato PDF aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-11/.

Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, **al informar campañas de phishing, malware y/o sitios fraudulentos.**

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono **1510** siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Bárbara Palacios Cabezas
- Macarena Alejandra Marco León
- Jhonnathan Alexis Vergara Alvarado
- Jamie
- Marcos Ramírez
- Fernando Graterol
- Felipe Ignacio Velozo Ruiz
- Felipe Flores Ruiz
- Manuel Velasco Silva
- Eduardo Retamales
- Felipe Andrés Mardones Mujica
- Nazih Minkara