Ministerio del Interior y Seguridad Pública

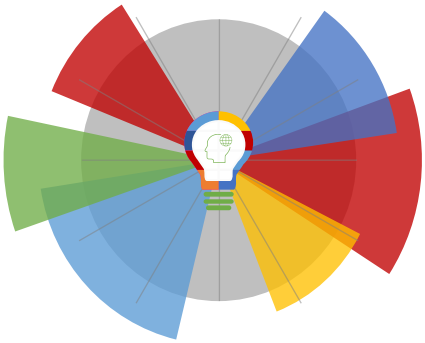
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

22-04-2022 | Año 4 | N°146

Boletín de Seguridad Cibernética

Semana del 14 al 21 de abril de 2022

La semana en cifras



Se advirtieron

8

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

249

para vulnerabilidades

Sus mitigaciones son útiles en productos de Apache, Oracle y Google.

IP

5

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

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob https://www.linkedin.com/company/csirt-gob

Sitios fraudulentos

Imagen del sitio

CSIRT informa sitio fraudulento del Banco Estado	
Alerta de seguridad cibernética	8FFR22-01075-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2022
Última revisión	19 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://sixthstartech[.]com/smschile/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[101.53.141.67]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01075-01/	
https://www.csirt.gob.cl/media/2022/04/8FFR22-01075-01.pdf	

Imagen del sitio

CSIRT informa página web falsa de Netflix	
Alerta de seguridad cibernética	8FFR22-01076-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2022
Última revisión	19 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://eurocontabilidade[.]net/Netflix/clientId1193721/login.php#signin=true	
IP	
[108.167.188.177]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01076-01/	
https://www.csirt.gob.cl/media/2022/04/8FFR22-01076-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing con falsos puntos del Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00512-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2022
Última revisión	19 de abril de 2022
Indicadores de compromiso	
URL redirección	
p://ec2-18-231-198-74.sa-east1.compute.amazonaws[.]com/54605333/?hash=aWluZGFAaW50ZXJpb3IuZ292LmNs	
URL sitio falso	
hXXps://puntosacanjua.oportunidadaprovechelos[.]com/App712f708/access.php?verify=AJZ94OTL AJZ9-XKXV-AJZ9XKXVXKXVHJXBXKXV&sessionUser=c5f4hdl3toumkb3pjnedlp3sgi&userLogin=6512bd43d9caa6e02c990b0a82652dca&queryString=	
IP	
[172.67.137.118]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00512-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00512-01.pdf	

Imagen del mensaje

CSIRT alerta phishing que proviene falsamente del Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00513-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2022
Última revisión	11 de abril de 2022
Indicadores de compromiso	
URL redirección	
hXXps://www.fabianofernandes.adm[.]br/wp-content/languages/–/https:/login.portal.bancochile.cl/?	
URL sitio falso	
hXXps://email-mipass[.]com/web/acesso.php	
IP	
[2.56.59.184]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00513-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00513-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FPH22-00514-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de abril de 2022
Última revisión	20 de abril de 2022
Indicadores de compromiso	
URL redirección	
hXXps://kendranew[.]com/activacion/cuenta-gkll/	
URL sitio falso	
hXXps://news.te[.}ua/sociedad/front/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[195.201.34.52]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00514-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00514-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en Apache Struts	
Alerta de seguridad cibernética	9VSA22-00620-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de abril de 2022
Última revisión	14 de abril de 2022
CVE	
CVE-2021-31805	
Fabricante	
Apache	
Productos afectados	
Apache Struts 2 2.0.0 a 2.5.29 (inclusive)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00620-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00620-01.pdf	

CSIRT alerta de vulnerabilidad en plugin Elementor de WordPress	
Alerta de seguridad cibernética	9VSA22-00621-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2022
Última revisión	19 de abril de 2022
CVE	
No cuenta con CVE	
Fabricante	
WordPress	
Productos afectados	
Elementor, versiones desde la 3.6.0 y anteriores a 3.6.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00621-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00621-01-1.pdf	

CSIRT alerta ante nueva vulnerabilidad en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00622-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de abril de 2022
Última revisión	19 de abril de 2022
CVE	
CVE-2022-1364	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones anteriores a 100.0.4896.127.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00622-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00622-01.pdf	

CSIRT alerta de actualización de seguridad de Oracle para abril 2022		
Alerta de seguridad cibernética	9VSA22-00623-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	20 de abril de 2022	
Última revisión	20 de abril de 2022	
CVE		
CVE-2017-1000353	CVE-2021-28657	CVE-2022-21425
CVE-2018-11212	CVE-2021-29425	CVE-2022-21426
CVE-2018-1285	CVE-2021-29921	CVE-2022-21427
CVE-2019-0227	CVE-2021-30129	CVE-2022-21430
CVE-2019-10086	CVE-2021-30468	CVE-2022-21431
CVE-2019-12086	CVE-2021-3156	CVE-2022-21434
CVE-2019-12399	CVE-2021-31812	CVE-2022-21435
CVE-2019-13565	CVE-2021-3200	CVE-2022-21436
CVE-2019-14862	CVE-2021-32066	CVE-2022-21437
CVE-2019-16789	CVE-2021-32626	CVE-2022-21438
CVE-2019-17195	CVE-2021-33037	CVE-2022-21440
CVE-2019-18276	CVE-2021-33813	CVE-2022-21441
CVE-2019-3740	CVE-2021-33880	CVE-2022-21442
CVE-2019-3799	CVE-2021-34429	CVE-2022-21443
CVE-2020-10878	CVE-2021-3450	CVE-2022-21444
CVE-2020-11022	CVE-2021-35043	CVE-2022-21445
CVE-2020-11612	CVE-2021-3518	CVE-2022-21446
CVE-2020-11971	CVE-2021-3520	CVE-2022-21447
CVE-2020-11979	CVE-2021-3521	CVE-2022-21448
CVE-2020-13434	CVE-2021-35515	CVE-2022-21449
CVE-2020-13936	CVE-2021-35574	CVE-2022-21450

CVE-2020-13956	CVE-2021-3572	CVE-2022-21451
CVE-2020-14155	CVE-2021-36090	CVE-2022-21452
CVE-2020-14340	CVE-2021-36090,	CVE-2022-21453
CVE-2020-14343	CVE-2021-36374	CVE-2022-21454
CVE-2020-15250	CVE-2021-3690	CVE-2022-21457
CVE-2020-16135	CVE-2021-3711	CVE-2022-21458
CVE-2020-17521	CVE-2021-3712	CVE-2022-21459
CVE-2020-17527	CVE-2021-37137	CVE-2022-21460
CVE-2020-17530	CVE-2021-37714	CVE-2022-21461
CVE-2020-1968	CVE-2021-3807	CVE-2022-21462
CVE-2020-1971	CVE-2021-38153	CVE-2022-21463
CVE-2020-24750	CVE-2021-39139	CVE-2022-21464
CVE-2020-24977	CVE-2021-39140	CVE-2022-21465
CVE-2020-25638	CVE-2021-39153	CVE-2022-21466
CVE-2020-25649	CVE-2021-39275	CVE-2022-21467
CVE-2020-27218	CVE-2021-40438	CVE-2022-21468
CVE-2020-28052	CVE-2021-40690	CVE-2022-21469
CVE-2020-28196	CVE-2021-41165	CVE-2022-21470
CVE-2020-29363	CVE-2021-41184	CVE-2022-21471
CVE-2020-29582	CVE-2021-4160	CVE-2022-21472
CVE-2020-35198	CVE-2021-41973	CVE-2022-21473
CVE-2020-36242	CVE-2021-42013	CVE-2022-21474
CVE-2020-36518	CVE-2021-42340	CVE-2022-21475
CVE-2020-5245	CVE-2021-42392	CVE-2022-21476
CVE-2020-5421	CVE-2021-43527	CVE-2022-21477
CVE-2020-6950	CVE-2021-43797	CVE-2022-21478
CVE-2020-7226	CVE-2021-43859	CVE-2022-21479
CVE-2020-7760	CVE-2021-44224	CVE-2022-21480
CVE-2020-8174	CVE-2021-44533	CVE-2022-21481
CVE-2020-8203	CVE-2021-44790	CVE-2022-21482
CVE-2020-8231	CVE-2021-44832	CVE-2022-21483
CVE-2020-8554	CVE-2022-0778	CVE-2022-21484
CVE-2020-8908	CVE-2022-20612	CVE-2022-21485
CVE-2020-9488	CVE-2022-20613	CVE-2022-21486
CVE-2021-20289	CVE-2022-20615	CVE-2022-21487
CVE-2021-21275	CVE-2022-21404	CVE-2022-21488
CVE-2021-21409	CVE-2022-21405	CVE-2022-21489
CVE-2021-22096	CVE-2022-21409	CVE-2022-21490
CVE-2021-22118	CVE-2022-21410	CVE-2022-21491
CVE-2021-22132	CVE-2022-21411	CVE-2022-21492
CVE-2021-22569	CVE-2022-21412	CVE-2022-21493
CVE-2021-22570	CVE-2022-21413	CVE-2022-21494
CVE-2021-22901	CVE-2022-21414	CVE-2022-21496
CVE-2021-22946	CVE-2022-21415	CVE-2022-21497
CVE-2021-23017	CVE-2022-21416	CVE-2022-21498
CVE-2021-23450	CVE-2022-21417	CVE-2022-22947
CVE-2021-2351	CVE-2022-21418	CVE-2022-22965
CVE-2021-2464	CVE-2022-21419	CVE-2022-23181
CVE-2021-2471	CVE-2022-21420	CVE-2022-23221

CVE-2021-26291	CVE-2022-21421	CVE-2022-23305
CVE-2021-28168	CVE-2022-21422	CVE-2022-23437
CVE-2021-28169	CVE-2022-21423	CVE-2022-23990
CVE-2021-28170	CVE-2022-21424	CVE-2022-2432
Vulnerabilidades críticas:		
CVE-2022-21410	CVE-2021-43527	CVE-2018-1285
CVE-2021-23017	CVE-2022-23221	CVE-2020-36242
CVE-2021-26291	CVE-2022-22965	CVE-2021-40438
CVE-2022-21431	CVE-2020-14343	CVE-2022-21420
CVE-2022-23305	CVE-2021-42392	CVE-2021-39275
CVE-2022-23990	CVE-2021-35574	CVE-2022-21445
CVE-2022-22947	CVE-2021-3520	CVE-2021-3711
CVE-2017-1000353	CVE-2020-17530	CVE-2021-42013
CVE-2022-22965	CVE-2021-44790	CVE-2019-17195
CVE-2021-29921	CVE-2021-23450	

Fabricante

Oracle

Productos afectados

Engineered Systems Utilities, versions 12.1.0.2, 19c, 21c
Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0
Enterprise Manager for Peoplesoft, versions 13.4.1.1, 13.5.1.1
Enterprise Manager for Storage Management, version 13.4.0.0
Enterprise Manager Ops Center, version 12.4.0.0
Helidon, versions 1.4.7, 1.4.10, 2.0.0-RC1
Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3
JD Edwards EnterpriseOne Tools, versions prior to 9.2.6.3
JD Edwards World Security, version A9.4
Management Cloud Engine, versions 1.5.0 and prior
Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
MySQL Cluster, versions 7.4.35 and prior, 7.5.25 and prior, 7.6.21 and prior, 8.0.28 and prior
MySQL Connectors, versions 8.0.28 and prior
MySQL Enterprise Monitor, versions 8.0.29 and prior
MySQL Server, versions 5.7.37 and prior, 8.0.28 and prior
MySQL Workbench, versions 8.0.28 and prior
Oracle Advanced Supply Chain Planning, versions 12.1, 12.2
Oracle Agile Engineering Data Management, version 6.2.1.0
Oracle Agile PLM, version 9.3.6
Oracle Agile PLM MCAD Connector, version 3.6
Oracle Application Express, versions prior to 22.1
Oracle Application Testing Suite, version 13.3.0.1
Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
Oracle Banking Deposits and Lines of Credit Servicing, version 2.12.0
Oracle Banking Enterprise Default Management, versions 2.7.1, 2.10.0, 2.12.0

Oracle Banking Loans Servicing, version 2.12.0
Oracle Banking Party Management, version 2.7.0
Oracle Banking Payments, version 14.5
Oracle Banking Platform, versions 2.6.2, 2.7.1, 2.12.0
Oracle Banking Trade Finance, version 14.5
Oracle Banking Treasury Management, version 14.5
Oracle Blockchain Platform, versions prior to 21.1.2
Oracle Business Intelligence Enterprise Edition, versions 5.5.0.0.0, 5.9.0.0.0, 12.2.1.3.0, 12.2.1.4.0
Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Coherence, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
Oracle Commerce Guided Search, version 11.3.2
Oracle Communications ASAP, version 7.3
Oracle Communications Billing and Revenue Management, versions 12.0.0.4, 12.0.0.5
Oracle Communications Cloud Native Core Automated Test Suite, versions 1.8.0, 1.9.0, 22.1.0
Oracle Communications Cloud Native Core Binding Support Function, version 1.11.0
Oracle Communications Cloud Native Core Console, versions 1.9.0, 22.1.0
Oracle Communications Cloud Native Core Network Exposure Function, version 22.1.0
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.10.0, 22.1.0
Oracle Communications Cloud Native Core Network Repository Function, versions 1.15.0, 1.15.1, 22.1.0
Oracle Communications Cloud Native Core Network Slice Selection Function, versions 1.8.0, 22.1.0
Oracle Communications Cloud Native Core Policy, versions 1.14.0, 1.15.0, 22.1.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 1.7.0, 22.1.0
Oracle Communications Cloud Native Core Service Communication Proxy, version 1.15.0
Oracle Communications Cloud Native Core Unified Data Repository, versions 1.15.0, 22.1.0
Oracle Communications Contacts Server, version 8.0.0.6.0
Oracle Communications Convergence, versions 3.0.2.2, 3.0.3.0
Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.4.0.0
Oracle Communications Design Studio, versions 7.3.5, 7.4.0-7.4.2
Oracle Communications Diameter Intelligence Hub, versions 8.0.0-8.2.3
Oracle Communications Diameter Signaling Router, version 8.4.0.0
Oracle Communications EAGLE Application Processor
Oracle Communications EAGLE Element Management System, version 46.6
Oracle Communications EAGLE FTP Table Base Retrieval, version 4.5
Oracle Communications EAGLE LNP Application Processor, versions 10.1,

10.2
Oracle Communications EAGLE Software, versions 46.7.0, 46.8.0-46.8.2, 46.9.1-46.9.3
Oracle Communications Element Manager, versions prior to 9.0
Oracle Communications Evolved Communications Application Server, version 7.1
Oracle Communications Instant Messaging Server, version 10.0.1.5.0
Oracle Communications Interactive Session Recorder, version 6.4
Oracle Communications IP Service Activator, version 7.4.0
Oracle Communications Messaging Server, version 8.1
Oracle Communications MetaSolv Solution, version 6.3.1
Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.4.0.0
Oracle Communications Network Integrity, versions 7.3.2, 7.3.5, 7.3.6
Oracle Communications Operations Monitor, versions 4.3, 4.4, 5.0
Oracle Communications Order and Service Management, versions 7.3, 7.4
Oracle Communications Performance Intelligence Center (PIC) Software, versions 10.3.0.0.0-10.3.0.2.1, 10.4.0.1.0-10.4.0.3.1
Oracle Communications Policy Management, versions 12.5.0.0.0, 12.6.0.0.0
Oracle Communications Pricing Design Center, versions 12.0.0.4, 12.0.0.5
Oracle Communications Services Gatekeeper, version 7.0.0.0.0
Oracle Communications Session Border Controller, versions 8.4, 9.0
Oracle Communications Session Report Manager, versions prior to 9.0
Oracle Communications Session Route Manager, versions prior to 9.0
Oracle Communications Unified Inventory Management, versions 7.4.1, 7.4.2
Oracle Communications Unified Session Manager, versions 8.2.5, 8.4.5
Oracle Communications User Data Repository, version 12.4
Oracle Communications WebRTC Session Controller, version 7.2.1
Oracle Data Integrator, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Database Server, versions 12.1.0.2, 19c, 21c
Oracle Documaker, versions 12.6.0, 12.6.2-12.6.4, 12.7.0
Oracle E-Business Suite, versions 12.2.4-12.2.11, [EBS Cloud Manager and Backup Module] prior to 22.1.1.1, [Enterprise Command Center] 7.0, [Enterprise Information Discovery] 7-9
Oracle Enterprise Communications Broker, versions 3.2, 3.3
Oracle Enterprise Session Border Controller, versions 8.4, 9.0
Oracle Ethernet Switch ES1-24, version 1.3.1
Oracle Ethernet Switch TOR-72, version 1.2.2
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.6.0-8.0.9.0, 8.1.0.0-8.1.2.0
Oracle Financial Services Behavior Detection Platform, versions 8.0.6.0-8.0.8.0, 8.1.1.0, 8.1.1.1, 8.1.2.0
Oracle Financial Services Enterprise Case Management, versions 8.0.7.1, 8.0.7.2, 8.0.8.0, 8.0.8.1, 8.1.1.0, 8.1.1.1, 8.1.2.0
Oracle Financial Services Revenue Management and Billing, versions 2.7.0.0, 2.7.0.1, 2.8.0.0

Oracle FLEXCUBE Universal Banking, versions 11.83.3, 12.1-12.4, 14.0-14.3, 14.5
Oracle Global Lifecycle Management OPatch
Oracle GoldenGate, versions prior to 12.3.0.1.2, prior to 23.1
Oracle GoldenGate Application Adapters, versions prior to 23.1
Oracle GoldenGate Big Data and Application Adapters, versions prior to 23.1
Oracle GraalVM Enterprise Edition, versions 20.3.5, 21.3.1, 22.0.0.2
Oracle Health Sciences Empirica Signal, versions 9.1.0.6, 9.2.0.0
Oracle Health Sciences InForm, versions 6.2.1.1, 6.3.2.1, 7.0.0.0
Oracle Health Sciences InForm Publisher, versions 6.2.1.1, 6.3.1.1
Oracle Health Sciences Information Manager, versions 3.0.1-3.0.4
Oracle Healthcare Data Repository, versions 8.1.0, 8.1.1
Oracle Healthcare Foundation, versions 7.3.0.1-7.3.0.4
Oracle Healthcare Master Person Index, version 5.0.1
Oracle Healthcare Translational Research, versions 4.1.0, 4.1.1
Oracle Hospitality Suite8, versions 8.10.2, 8.11.0-8.14.0
Oracle Hospitality Token Proxy Service, version 19.2
Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Hyperion BI+, versions prior to 11.2.8.0
Oracle Hyperion Calculation Manager, versions prior to 11.2.8.0
Oracle Hyperion Data Relationship Management, versions prior to 11.2.8.0, prior to 11.2.9.0
Oracle Hyperion Financial Management, versions prior to 11.2.8.0
Oracle Hyperion Infrastructure Technology, versions prior to 11.2.8.0
Oracle Hyperion Planning, versions prior to 11.2.8.0
Oracle Hyperion Profitability and Cost Management, versions prior to 11.2.8.0
Oracle Hyperion Tax Provision, versions prior to 11.2.8.0
Oracle Identity Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Identity Manager Connector, versions 9.1.0, 11.1.1.5.0
Oracle iLearning, versions 6.2, 6.3
Oracle Insurance Data Gateway, version 1.0.1
Oracle Insurance Insbridge Rating and Underwriting, versions 5.2.0, 5.4.0-5.6.0, 5.6.1
Oracle Insurance Policy Administration, versions 11.0.2, 11.1.0, 11.2.8, 11.3.0, 11.3.1
Oracle Insurance Rules Palette, versions 11.0.2, 11.1.0, 11.2.8, 11.3.0, 11.3.1
Oracle Internet Directory, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Java SE, versions 7u331, 8u321, 11.0.14, 17.0.2, 18
Oracle JDeveloper, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Managed File Transfer, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Middleware Common Libraries and Tools, version 12.2.1.4.0
Oracle NoSQL Database
Oracle Outside In Technology, version 8.5.5
Oracle Payment Interface, versions 19.1, 20.3
Oracle Product Lifecycle Analytics, version 3.6.1.0
Oracle REST Data Services, versions prior to 21.2

Oracle Retail Bulk Data Integration, version 16.0.3 Oracle Retail Customer Insights, versions 15.0.2, 16.0.2 Oracle Retail Customer Management and Segmentation Foundation, versions 17.0-19.0 Oracle Retail Data Extractor for Merchandising, versions 15.0.2, 16.0.2 Oracle Retail EFTLink, versions 17.0.2, 18.0.1, 19.0.1, 20.0.1, 21.0.0 Oracle Retail Extract Transform and Load, version 13.2.8 Oracle Retail Financial Integration, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1 Oracle Retail Integration Bus, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1 Oracle Retail Invoice Matching, version 16.0.3 Oracle Retail Merchandising System, versions 16.0.3, 19.0.1 Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.1-16.0.3, 19.0.0, 19.0.1 Oracle Retail Store Inventory Management, versions 14.0.4.13, 14.1.3.5, 14.1.3.14, 15.0.3.3, 15.0.3.8, 16.0.3.7 Oracle Retail Xstore Office Cloud Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1 Oracle Retail Xstore Point of Service, versions 16.0.6, 17.0.4, 18.0.3, 19.0.2, 20.0.1, 21.0.0 Oracle SD-WAN Edge, versions 9.0, 9.1 Oracle Secure Backup Oracle Secure Global Desktop, version 5.6 Oracle Solaris, version 11 Oracle Solaris Cluster, version 4 Oracle SQL Developer, versions prior to 21.99 Oracle StorageTek ACSLS, version 8.5.1 Oracle StorageTek Tape Analytics (STA), version 2.4 Oracle Taleo Platform, versions prior to 22.1 Oracle Transportation Management, versions 6.4.3, 6.5.1 Oracle Tuxedo, version 12.2.2.0.0 Oracle Utilities Framework, versions 4.3.0.1.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0 Oracle VM VirtualBox, versions prior to 6.1.34 Oracle Web Services Manager, versions 12.2.1.3.0, 12.2.1.4.0 Oracle WebCenter Portal, versions 12.2.1.3.0, 12.2.1.4.0 Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0 Oracle WebLogic Server, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 Oracle ZFS Storage Appliance Kit, version 8.8 OSS Support Tools, versions 2.12.42, 18.3 PeopleSoft Enterprise CS Academic Advisement, version 9.2 PeopleSoft Enterprise FIN Cash Management, version 9.2 PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59 PeopleSoft Enterprise PRTL Interaction Hub, version 9.1 Primavera Unifier, versions 17.7-17.12, 18.8, 19.12, 20.12, 21.12
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00623-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00623-01.pdf

Actualidad

Ciberdiccionario Volumen 2

El CSIRT de Gobierno compartió esta semana el volumen n°2 del Ciberdiccionario, el cual entrega definiciones simples y sencillas con términos relacionados con la ciberseguridad. El objetivo de esta nueva campaña es acercar el mundo informático a todos los ciudadanos, de manera de comprender los riesgos y formas de protección.

En este segundo volumen explicamos qué significan los conceptos CSIRT, firewall, malware, cifrado y vulnerabilidades. Pueden verlo también en: csirt.gob.cl/recomendaciones/ciberdiccionario-vol-2/

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Juan Alfonso Muñoz
- César López
- Felipe Pizarro
- Christian Abarca
- Bárbara Palacios
- Juan Downey
- Cristián Acuña
- Juan Alejandro Muñoz
- Hanz Sandoval
- José Antonio Berríos
- David Soto
- Carlos Escalona