CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 251

semana del 19 al 25 de abril de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

6

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

9

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

300

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

HASH REPORTADOS

2

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware.

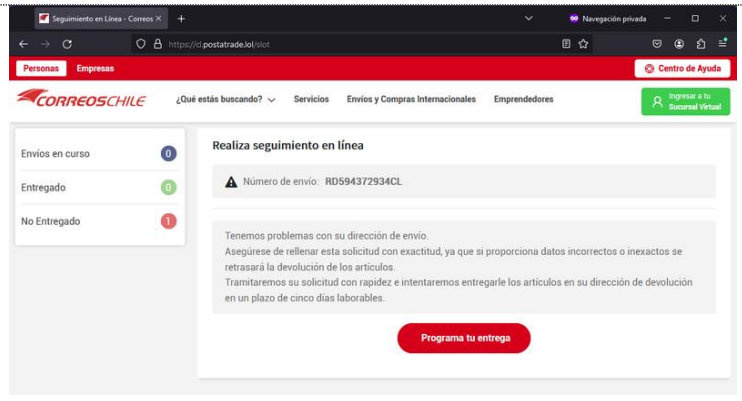
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

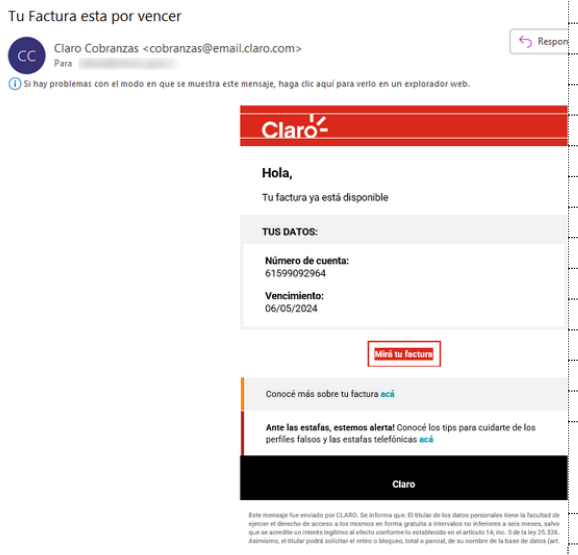
Blue Express - Falsificación	
Código de alerta	FFR24-01680
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2024
Última revisión	23 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://blueexpress.superman-url.buzz/slot	
Dirección IP sitio falso	
[162.62.53.33]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01680/	

Blue Express - Falsificación	
Código de alerta	FFR24-01681
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2024
Última revisión	23 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://blueexpress.duck-url.buzz/slot	
Dirección IP sitio falso	
[162.62.53.33]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01681/	



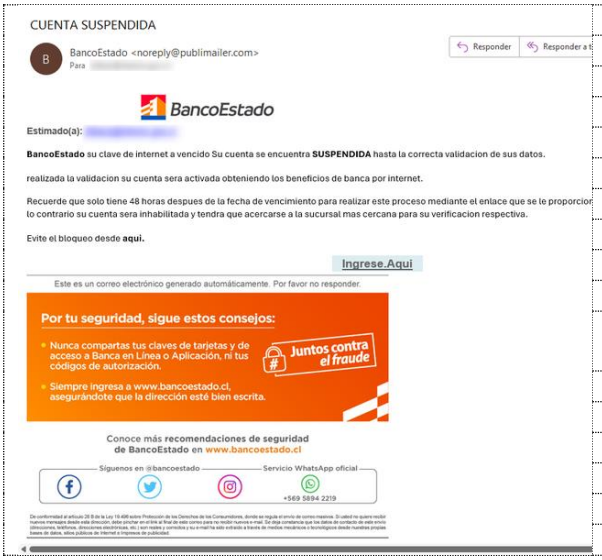
CorreosChile - Falsificación	
Código de alerta	FFR24-01682
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2024
Última revisión	23 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://cl.postatrade.lol/slot	
Dirección IP sitio falso	
[162.62.53.33]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8ffr24-01682/	

3. Malware

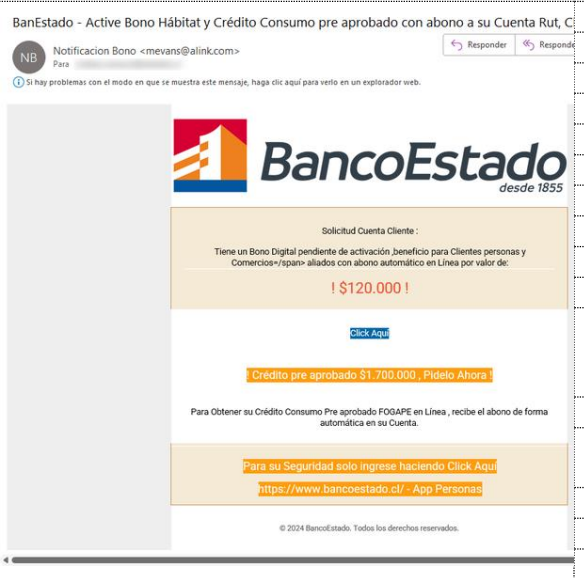


Claro - Suplantación con malware	
Código de alerta	CMV24-00459
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de abril de 2024
Última revisión	24 de abril de 2024
Indicadores de compromiso	
Asunto	
Tu factura esta por vencer	
Correo de salida	
cobranzas@email.claro.com	
SHA256	
4c03891763e6c40c8610017c97a2611d8a4178803eee14b2fc7749819020168b f05ca75ef01264185e8669b7818de091fc06d574deecc5af07f5645314e380cd	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/cmv24-00459/	

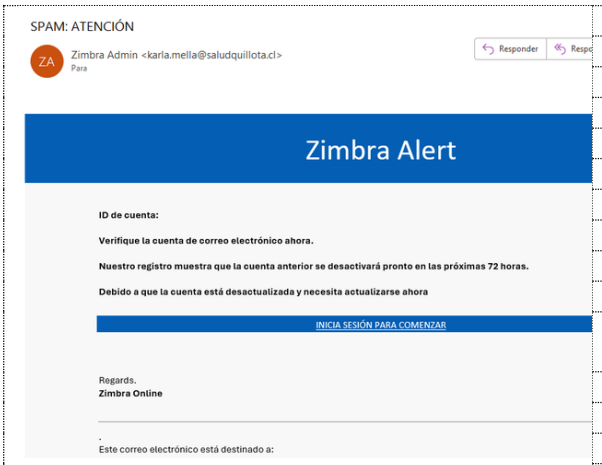
4. Phishing



BancoEstado - Phishing	
Alerta de seguridad cibernética	FPH24-00953
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de abril de 2024
Última revisión	22 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://fogape.larissakovalchuk.com/1713799490/imagenes/_personas/home/default.asp	
URL de redirección	
https://temucoproduce.com/activacion/cuenta-nldo/	
Dirección IP sitio falso	
[122.201.66.57]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00953/	

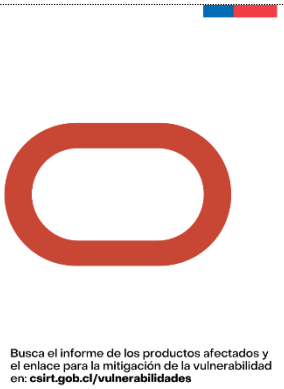


BancoEstado - Phishing	
Alerta de seguridad cibernética	FPH24-00954
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de abril de 2024
Última revisión	23 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://portal-digitalbonobancooestado.pages.dev/?cvid=rja&CNhFD5ilyYGk6vBMtfgSpweUq8bQ3EXHoPLIaJcAZzV1sxTWrO9740ujmdKRn2	
URL de redirección	
http://159.65.156.91/dc8a63028568ce934158852be92c13c9/db44ec749ab06ea44c53S/5ead2be--f8a12a42bb492/?k=KERT	
https://bit.ly/4cBQnRD	
Dirección IP sitio falso	
[172.66.47.116]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00954/	



Zimbra - Phishing	
Alerta de seguridad cibernética	FPH24-00955
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2024
Última revisión	25 de abril de 2024
Indicadores de compromiso	
URL del sitio falso	
https://ipfs.io/ipfs/bafybeih4wwljr3lg6fxunpfgmjpqlwhihybtxvvbn5wesic6ii6wdjizfm/eso.com.mk.htm	
Dirección IP sitio falso	
[209.94.90.1]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/fph24-00955/	

5. Vulnerabilidades



Oracle Update Abril 2024 - Vulnerabilidades	
Código de alerta	VSA24-01004
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de abril de 2024
Última revisión	18 de abril de 2024

CVE y puntaje CVSS

CVE-2024-20997	9.9	CVE-2024-21019	6.1
CVE-2024-21010	9.9	CVE-2024-21020	6.1
CVE-2022-46364	9.8	CVE-2024-21021	6.1
CVE-2023-47100	9.8	CVE-2024-21022	6.1
CVE-2022-34381	9.8	CVE-2024-21023	6.1
CVE-2022-42920	9.8	CVE-2024-21024	6.1
CVE-2022-46337	9.8	CVE-2024-21025	6.1
CVE-2024-21014	9.8	CVE-2024-21026	6.1
CVE-2024-1597	9.8	CVE-2024-21027	6.1
CVE-2019-13990	9.8	CVE-2024-21028	6.1
CVE-2022-1471	9.8	CVE-2024-21029	6.1
CVE-2022-45378	9.8	CVE-2024-21030	6.1
CVE-2021-23369	9.8	CVE-2024-21031	6.1
CVE-2024-21082	9.8	CVE-2024-21032	6.1
CVE-2022-42889	9.8	CVE-2024-21033	6.1
CVE-2023-38545	9.8	CVE-2024-21034	6.1
CVE-2020-35168	9.8	CVE-2024-21035	6.1
CVE-2024-21071	9.1	CVE-2024-21036	6.1
CVE-2023-43496	8.8	CVE-2024-21037	6.1
CVE-2023-4863	8.8	CVE-2024-21038	6.1
CVE-2024-21067	8.8	CVE-2024-21039	6.1
CVE-2023-46604	8.8	CVE-2024-21040	6.1
CVE-2023-37536	8.8	CVE-2024-21041	6.1
CVE-2024-21112	8.8	CVE-2024-21042	6.1
CVE-2024-21113	8.8	CVE-2024-21043	6.1
CVE-2024-21114	8.8	CVE-2024-21044	6.1
CVE-2024-21115	8.8	CVE-2024-21045	6.1
CVE-2024-21626	8.6	CVE-2024-21046	6.1
CVE-2024-22257	8.2	CVE-2024-21072	6.1
CVE-2024-21095	8.2	CVE-2024-23635	6.1
CVE-2024-20999	8.2	CVE-2022-31160	6.1
CVE-2024-22259	8.1	CVE-2024-24816	6.1
CVE-2023-41056	8.1	CVE-2024-21063	6.1
CVE-2023-44981	8.1	CVE-2024-21065	6.1
CVE-2023-43804	8.1	CVE-2022-36033	6.1
CVE-2024-21092	8.1	CVE-2023-48795	5.9
CVE-2023-51257	7.8	CVE-2024-21109	5.9
CVE-2021-36770	7.8	CVE-2024-21084	5.8
CVE-2023-6246	7.8	CVE-2023-0833	5.5
CVE-2021-43113	7.8	CVE-2024-26308	5.5
CVE-2023-4807	7.8	CVE-2023-4641	5.5
CVE-2024-21059	7.8	CVE-2022-40896	5.5

	CVE-2024-21103	7.8	CVE-2023-5341	5.5
	CVE-2024-21111	7.8	CVE-2023-42503	5.5
	CVE-2024-21116	7.8	CVE-2023-29081	5.5
	CVE-2023-46589	7.5	CVE-2024-21015	5.5
	CVE-2023-1370	7.5	CVE-2022-24613	5.5
	CVE-2022-42003	7.5	CVE-2021-36374	5.5
	CVE-2023-44487	7.5	CVE-2024-22243	5.4
	CVE-2023-34053	7.5	CVE-2024-21064	5.4
	CVE-2024-21634	7.5	CVE-2024-21001	5.4
	CVE-2023-4043	7.5	CVE-2024-21070	5.4
	CVE-2023-6378	7.5	CVE-2024-21070	5.4
	CVE-2022-34169	7.5	CVE-2024-21093	5.3
	CVE-2024-26130	7.5	CVE-2023-51074	5.3
	CVE-2024-22201	7.5	CVE-2023-33201	5.3
	CVE-2022-40152	7.5	CVE-2024-20990	5.3
	CVE-2023-49083	7.5	CVE-2022-24329	5.3
	CVE-2024-22233	7.5	CVE-2024-20991	5.3
	CVE-2023-45142	7.5	CVE-2024-21119	5.3
	CVE-2024-25062	7.5	CVE-2024-21117	5.3
	CVE-2023-5363	7.5	CVE-2024-21120	5.3
	CVE-2024-1635	7.5	CVE-2024-21118	5.3
	CVE-2022-45688	7.5	CVE-2023-3817	5.3
	CVE-2023-51775	7.5	CVE-2024-0853	5.3
	CVE-2023-31122	7.5	CVE-2024-20994	5.3
	CVE-2023-52428	7.5	CVE-2024-21058	4.9
	CVE-2024-21078	7.5	CVE-2023-6507	4.9
	CVE-2024-21079	7.5	CVE-2024-21102	4.9
	CVE-2024-21088	7.5	CVE-2024-21047	4.9
	CVE-2024-21073	7.5	CVE-2024-21061	4.9
	CVE-2024-21074	7.5	CVE-2024-21069	4.9
	CVE-2024-21075	7.5	CVE-2024-21049	4.9
	CVE-2024-21076	7.5	CVE-2024-21050	4.9
	CVE-2024-21077	7.5	CVE-2024-21051	4.9
	CVE-2023-2618	7.5	CVE-2024-21052	4.9
	CVE-2023-44271	7.5	CVE-2024-21053	4.9
	CVE-2019-0231	7.5	CVE-2024-21056	4.9
	CVE-2023-24021	7.5	CVE-2024-21060	4.9
	CVE-2019-10172	7.5	CVE-2024-21087	4.9
	CVE-2023-3635	7.5	CVE-2024-21056	4.9
	CVE-2024-21006	7.5	CVE-2024-21060	4.9
	CVE-2024-21007	7.5	CVE-2024-21087	4.9
	CVE-2022-42890	7.5	CVE-2024-20993	4.9
	CVE-2024-21892	7.5	CVE-2024-20998	4.9
	CVE-2024-21892	7.5	CVE-2024-21009	4.9
	CVE-2023-41993	7.5	CVE-2024-21054	4.9
	CVE-2024-21090	7.5	CVE-2024-21055	4.9
	CVE-2023-1436	7.5	CVE-2024-21057	4.9
	CVE-2023-34981	7.5	CVE-2024-21062	4.9
	CVE-2023-24998	7.5	CVE-2024-21096	4.9
	CVE-2022-24839	7.5	CVE-2024-21097	4.9
	CVE-2021-28861	7.4	CVE-2024-21081	4.7
	CVE-2020-25638	7.4	CVE-2023-35116	4.9
	CVE-2024-21110	7.3	CVE-2024-20992	4.4
	CVE-2024-21083	7.2	CVE-2024-21008	4.4
	CVE-2021-41616	7.2	CVE-2024-21013	4.4

CVE-2023-2976	7.1	CVE-2023-5072	4.3
CVE-2024-20989	7.0	CVE-2024-21086	4.3
CVE-2022-41853	6.7	CVE-2024-21048	4.3
CVE-2024-21107	6.7	CVE-2023-35887	4.3
CVE-2023-20863	6.5	CVE-2024-21099	4.3
CVE-2021-37533	6.5	CVE-2024-21066	4.2
CVE-2023-34055	6.5	CVE-2024-21100	4.0
CVE-2023-2283	6.5	CVE-2024-21000	3.8
CVE-2024-21080	6.5	CVE-2024-20954	3.7
CVE-2024-21089	6.5	CVE-2024-21098	3.7
CVE-2023-20861	6.5	CVE-2024-21085	3.7
CVE-2023-44483	6.5	CVE-2024-21011	3.7
CVE-2022-25147	6.5	CVE-2024-21068	3.7
CVE-2023-46218	6.5	CVE-2024-21094	3.7
CVE-2023-6129	6.5	CVE-2024-21012	3.7
CVE-2024-21091	6.5	CVE-2023-36632	3.5
CVE-2024-21104	6.5	CVE-2023-4016	3.5
CVE-2024-21106	6.5	CVE-2024-21108	3.3
CVE-2024-21121	6.5	CVE-2024-21003	3.1
CVE-2023-50386	6.3	CVE-2024-21005	3.1
CVE-2022-48579	6.2	CVE-2024-21002	2.5
CVE-2023-41080	6.1	CVE-2024-21004	2.5
CVE-2024-21016	6.1	CVE-2024-20995	2.4
CVE-2024-21017	6.1	CVE-2024-21101	2.2
CVE-2024-21018	6.1	CVE-2024-21105	2.0

Fabricante

Oracle

Productos afectados

Autonomous Health Framework Anteriores a 24.2
GraalVM Multilingual Engine 21.3-21.13
Grid Infrastructure (Apache Mina SSHD) 21.3-21.13
Java VM 19.3-19.22, 21.3-21.13
Management Cloud Engine 24.1.0.0.0
MySQL Cluster 7.5.33 y anteriores, 7.6.29 y anteriores, 8.0.36 y anteriores, 8.3.0 y anteriores
MySQL Cluster 8.0.36 y anteriores, 8.3.0 y anteriores
MySQL Connectors 8.3.0 y anteriores
MySQL Enterprise Backup 8.0.36 y anteriores, 8.3.0 y anteriores
MySQL Enterprise Monitor 8.0.37 y anteriores
MySQL Server 8.0.34 y anteriores, 8.3.0 y anteriores
MySQL Server 8.0.36 y anteriores, 8.3.0 y anteriores
OPatchAuto Anteriores a 12.2.0.1.42
Oracle Access Manager 12.2.1.4.0
Oracle Agile PLM 9.3.6
Oracle Agile Product Lifecycle Management for Process 6.2.4.2
Oracle Application Testing Suite 13.3.0.1
Oracle Applications Framework 12.2.9-12.2.13
Oracle Applications Technology 12.2.3-12.2.13
Oracle Banking APIs 19.1.0.0.0, 19.2.0.0.0, 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
Oracle Banking Branch 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
Oracle Banking Cash Management 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0
Oracle Banking Deposits and Lines of Credit Servicing 2.12.0.0.0

	Oracle Banking Digital Experience 19.1.0.0.0, 19.2.0.0.0, 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0 Oracle Banking Enterprise Default Management 2.7.0.0.0, 2.12.0.0.0 Oracle Banking Liquidity Management 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0 Oracle Banking Liquidity Management 14.7.0.3.0 Oracle Banking Loans Servicing 2.12.0.0.0 Oracle Banking Origination 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0 Oracle Banking Party Management 2.7.0.0.0 Oracle Banking Platform 2.12.0.0.0 Oracle Banking Platform 2.7.0.0.0 Oracle Banking Virtual Account Management 14.5.0.0.0, 14.6.0.0.0, 14.7.0.0.0 Oracle BI Publisher 7.0.0.0.0, 12.2.1.4.0 Oracle Big Data Spatial and Graph 3.0.5 Oracle Business Intelligence Enterprise Edition 12.2.1.4.0 Oracle Business Intelligence Enterprise Edition 7.0.0.0.0, 12.2.1.4.0 Oracle Coherence 12.2.1.4.0, 14.1.1.0.0 Oracle Commerce Guided Search 11.3.2 Oracle Commerce Platform 11.3.0, 11.3.1, 11.3.2 Oracle Communications Billing and Revenue Management 12.0.0.4-12.0.0.8, 15.0.0.0 Oracle Communications BRM - Elastic Charging Engine 12.0.0.4-12.0.0.8, 15.0.0.0 Oracle Communications Cloud Native Core Binding Support Function 23.4.0-23.4.2 Oracle Communications Cloud Native Core Console 23.4.0 Oracle Communications Cloud Native Core Network Data Analytics Function 24.1.0 Oracle Communications Cloud Native Core Network Exposure Function 23.4.1 Oracle Communications Cloud Native Core Network Function Cloud Native Environment 23.2.0, 23.3.1, 23.4.0 Oracle Communications Cloud Native Core Network Function Cloud Native Environment 23.4.0 Oracle Communications Cloud Native Core Network Repository Function 23.4.1 Oracle Communications Cloud Native Core Network Slice Selection Function 23.2.0, 23.3.0 Oracle Communications Cloud Native Core Policy 23.4.0-23.4.2 Oracle Communications Cloud Native Core Security Edge Protection Proxy 23.3.0 Oracle Communications Cloud Native Core Security Edge Protection Proxy 23.4.0 Oracle Communications Cloud Native Core Service Communication Proxy 23.1.0 Oracle Communications Cloud Native Core Service Communication Proxy 23.2.2 Oracle Communications Cloud Native Core Service Communication Proxy 23.3.0 Oracle Communications Cloud Native Core Unified Data Repository 22.4.0, 23.1.0, 23.2.0

	Oracle Communications Cloud Native Core Unified Data Repository 23.2.0 Oracle Communications Cloud Native Core Unified Data Repository 23.3.2 Oracle Communications Diameter Signaling Router 9.0.0.0 Oracle Communications Element Manager 9.0.0-9.0.2 Oracle Communications Fraud Monitor 5.0, 5.1, 5.2 Oracle Communications Network Integrity 7.3.6.4 Oracle Communications Offline Mediation Controller 12.0.0.1-12.0.0.8 Oracle Communications Operations Monitor 5.1, 5.2 Oracle Communications Service Catalog and Design 8.0.0.1.0 Oracle Communications Session Report Manager 9.0.0-9.0.2 Oracle Communications Unified Inventory Management 7.4.0-7.4.2, 7.5.0, 7.5.1 Oracle Communications User Data Repository 14.0.0.0.0 Oracle Communications WebRTC Session Controller 7.2.0.0.0-7.2.1.0.0 Oracle Complex Maintenance, Repair, and Overhaul 12.2.3-12.2.13 Oracle Concurrent Processing 12.2.3-12.2.13 Oracle CRM Technical Foundation 12.2.3-12.2.13 Oracle Data Integrator 12.2.1.4.0 Oracle Database Sharding 19.3-19.22, 21.3-21.13 Oracle Documaker 12.6, 12.7 Oracle Enterprise Data Quality 12.2.1.4.0 Oracle Enterprise Manager Base Platform 13.5.0.0 Oracle Enterprise Manager for Fusion Middleware 13.5.0.0 Oracle Financial Services Revenue Management and Billing 2.8.0.0.0, 2.9.0.0.0, 2.9.0.1.0, 3.0.0.0.0, 3.1.0.0.0, 3.2.0.0.0, 4.0.0.0, 5.0.0.0 Oracle Financial Services Revenue Management and Billing 3.2.0.0.0 Oracle FLEXCUBE Private Banking 12.1.0.0.0 Oracle Fusion Middleware MapViewer 12.2.1.4.0 Oracle Global Lifecycle Management NextGen OUI Framework 12.2.1.4.0 Oracle GoldenGate Stream Analytics 19.1.0.0.0-19.1.0.0.8 Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13, 21.3.9 Oracle GraalVM for JDK Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22 Oracle Healthcare Data Repository 8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.3.0, 8.1.3.2, 8.1.3.4 Oracle Hospitality Cruise Shipboard Property Management System 20.3.3, 20.3.4, 23.1.0, 23.1.1 Oracle Hospitality Simphony 19.1.0-19.5.4 Oracle HTTP Server 12.2.1.4.0 Oracle HTTP Server 12.2.1.4.0, 14.1.1.0.0 Oracle Hyperion Infrastructure Technology 11.2.16.0.000 Oracle Identity Manager Connector 12.2.1.3.0 Oracle Identity Manager 12.2.1.4.0 Oracle Installed Base 12.2.3-12.2.13 Oracle Internet Directory 12.2.1.4.0

	Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle Java SE: 8u401, 8u401-perf, 11.0.22; Oracle GraalVM Enterprise Edition: 20.3.13, 21.3.9 Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle Java SE: 8u401; Oracle GraalVM Enterprise Edition: 20.3.13, 21.3.9 Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition Oracle Java SE: 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13, 21.3.9 Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition Oracle Java SE: 8u401, 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13, 21.3.9 Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition Oracle Java SE: 8u401-perf, 11.0.22, 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 21.3.9 Oracle Life Sciences Empirica Signal 9.1.0.53, 9.2.0.53 Oracle Managed File Transfer 12.2.1.4.0 Oracle Marketing 12.2.3-12.2.13 Oracle Middleware Common Libraries and Tools 12.2.1.4.0, 14.1.1.0.0 Oracle Outside In Technology 8.5.6, 8.5.7 Oracle Partner Management 12.2.3-12.2.13 Oracle Production Scheduling 12.2.4-12.2.12 Oracle Retail Assortment Planning 15.0.3, 16.0.3 Oracle Retail Customer Management and Segmentation Foundation 19.0.0.9 Oracle Retail Integration Bus 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1 Oracle Retail Integration Bus 16.0.3, 19.0.1 Oracle Retail Merchandising System 14.1.3, 15.0.3, 16.0.3, 19.0.1 Oracle Retail Sales Audit 14.1.3.1, 15.0.3.1, 16.0.3, 19.0.1 Oracle Retail Service Backbone 14.1.3.2, 15.0.3.1, 16.0.3, 19.0.1 Oracle Retail Xstore Point of Service 19.0.5, 20.0.4, 21.0.3, 22.0.1, 23.0.1 Oracle SD-WAN Edge 9.1.1.7.0 Oracle Smart View for Office 11.2.16.0.000 Oracle SOA Suite 12.2.1.4.0 Oracle Solaris Cluster 4 Oracle Solaris 11 Oracle SQLcl (Apache Mina SSHD) 19.3-19.22, 21.3-21.13 Oracle StorageTek Tape Analytics (STA) 2.5 Oracle Trade Management 12.2.3-12.2.13 Oracle Transportation Management 6.5.2 Oracle Transportation Management 6.5.2, 6.5.3 Oracle Utilities Application Framework 4.3.0.3.0-4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.5.0.0.0, 4.5.0.1.1, 4.5.0.1.2 Oracle Utilities Network Management System 2.5.0.1, 2.5.0.2, 2.6.0.0, 2.6.0.1 Oracle VM VirtualBox Anteriores a 7.0.16 Oracle Web Applications Desktop Integrator 12.2.3-12.2.13 Oracle Web Services Manager 12.2.1.4.0 Oracle WebCenter Content 12.2.1.4.0 Oracle WebCenter Enterprise Capture 12.2.1.4.0 Oracle WebCenter Portal 12.2.1.4.0

	Oracle WebLogic Server 12.2.1.4.0, 14.1.1.0.0 Oracle WebLogic Server 14.1.1.0.0 Oracle Workflow 12.2.3-12.2.13 Oracle ZFS Storage Appliance Kit 8.8 OSS Support Tools 2.12.44 OSS Support Tools 2.12.45 OSS Support Tools 23.1.23.1.17 OSS Support Tools 24.1.24.1.16 PeopleSoft Enterprise CRM Client Management 9.2 PeopleSoft Enterprise HCM Benefits Administration 9.2 PeopleSoft Enterprise PeopleTools 8.59, 8.60, 8.61 PeopleSoft Enterprise PeopleTools 8.61 Primavera Gateway 19.12.0-19.12.18, 20.12.0-20.12.13, 21.12.0-21.12.11 Primavera P6 Enterprise Project Portfolio Management 19.12.0-19.12.22, 20.12.0-20.12.21, 21.12.0-21.12.18, 22.12.0-22.12.12, 23.12.0-23.12.2 Primavera Unifier 19.12.0-19.12.16, 20.12.0-20.12.16, 21.12.0-21.12.17, 22.12.0-22.12.12, 23.12.0-23.12.3 Product Supported Versions Affected RDBMS (Python) 21.3-21.13 RDBMS 19.3-19.22, 21.3-21.13 Siebel Apps - Public Sector 24.2 y anteriores Unified Audit 19.3-19.22, 21.3-21.13
	Enlaces para revisar el informe:
	https://csirt.gob.cl/alertas/vsa24-01004/

VMware ESXi y otros - Vulnerabilidades		
Código de alerta		VSA24-01005
Clase de alerta		Vulnerabilidad
Tipo de incidente		Sistema y/o Software Abierto
Nivel de riesgo		Alto
TLP		Blanco
Fecha de lanzamiento original		23 de abril de 2024
Última revisión		23 de abril de 2024
CVE, CVSS y EPSS		
CVE-2021-21974	8.8	35,63%
CVE-2019-5544	9.8	3.27%
CVE-2020-3992	9.8	87,96%
Fabricante		
VMware		
Productos afectados		
VMware ESXi • 7.0 before ESXi70U1c-17325551 • 6.7 before ESXi670-202102401-SG • 6.5 before ESXi650-202102101-SG VMware Cloud Foundation • 4.x before 4.2 and 3.x		
Enlaces para revisar el informe:		
https://csirt.gob.cl/alertas/vsa24-01005/		

Cisco - Vulnerabilidades	
Código de alerta	VSA24-01006
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2024
Última revisión	25 de abril de 2024

CVE, CVSS y EPSS		
CVE-2024-20295	8.8	0,04%
CVE-2024-20356	8.7	0,04%
CVE-2024-20353	8.6	1,18%
CVE-2024-20359	6.0	1,18%
CVE-2024-20358	6.0	0,04%

Fabricante

Cisco

Productos afectados

Cisco ASA Software
Cisco FTD Software
Cisco IMC

Enlaces para revisar el informe:

https://csirt.gob.cl/alertas/vsa24-01006/

Ivanti Avalanche - Vulnerabilidades	
Código de alerta	VSA24-01007
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2024
Última revisión	25 de abril de 2024

CVE, CVSS

CVE-2024-22061	8.1	CVE-2024-24994	8.8
CVE-2024-23526	5.3	CVE-2024-24995	8.8
CVE-2024-23527	5.3	CVE-2024-24996	9.8
CVE-2024-23528	5.3	CVE-2024-24997	8.8
CVE-2024-23529	5.3	CVE-2024-24998	8.8
CVE-2024-23530	5.3	CVE-2024-24999	8.8
CVE-2024-23531	7.5	CVE-2024-25000	8.8
CVE-2024-23533	4.3	CVE-2024-27975	8.8
CVE-2024-23532	7.5	CVE-2024-27976	8.8
CVE-2024-23534	8.8	CVE-2024-27977	7.1
CVE-2024-23535	8.8	CVE-2024-27978	6.5
CVE-2024-24991	6.5	CVE-2024-27984	7.1
CVE-2024-24992	8.8	CVE-2024-29204	9.8
CVE-2024-24993	8.8		

Fabricante

Ivanti

Productos afectados

Ivanti Avalanche anteriores a 6.4.3

Enlaces para revisar el informe:

https://csirt.gob.cl/alertas/vsa24-01007/

Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: **csirt.gob.cl/vulnerabilidades**

Google Chrome - Vulnerabilidades		
Código de alerta		VSA24-01008
Clase de alerta		Vulnerabilidad
Tipo de incidente		Sistema y/o Software Abierto
Nivel de riesgo		Alto
TLP		Blanco
Fecha de lanzamiento original		25 de abril de 2024
Última revisión		25 de abril de 2024
CVE, CVSS y EPSS		
CVE-2024-3832		0.05%
CVE-2024-3833		0.05%
CVE-2024-3914		0.05%
CVE-2024-3834	8.8	0.06%
CVE-2024-3837	8.8	0.06%
CVE-2024-3838	5.5	0.05%
CVE-2024-3839	6.5	0.05%
CVE-2024-3840		0.05%
CVE-2024-3841		0.05%
CVE-2024-3843		0.05%
CVE-2024-3844		0.05%
CVE-2024-3845		0.05%
CVE-2024-3846		0.05%
CVE-2024-3847		0.05%
Fabricante		
Google		
Productos afectados		
Google Chrome anterior a la version 124.0.6367.60/.61		
Enlaces para revisar el informe:		
https://csirt.gob.cl/alertas/vsa24-01008/		

Busca el informe de los productos afectados y el enlace para la mitigación de la vulnerabilidad en: **csirt.gob.cl/vulnerabilidades**

Mozilla Firefox - Vulnerabilidades	
Código de alerta	VSA24-01009
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de abril de 2024
Última revisión	25 de abril de 2024
CVE y EPSS	
CVE-2024-3852	0.05%
CVE-2024-3853	0.04%
CVE-2024-3854	0.05%
CVE-2024-3855	0.04%
CVE-2024-3856	0.04%
CVE-2024-3857	0.05%
CVE-2024-3858	0.04%
CVE-2024-3859	0.05%
CVE-2024-3860	0.04%
CVE-2024-3861	0.05%
CVE-2024-3862	0.04%
CVE-2024-3863	0.05%
Fabricante	
Mozilla	

	Productos afectados
	Mozilla Firefox Anterior a 125 Mozilla Firefox ESX Anterior a 115.10. Mozilla Thunderbird Anterior a 115.10.
	Enlaces para revisar el informe:
	https://csirt.gob.cl/alertas/vsa24-01009/

4. Noticias y concientización

Equipo de la Coordinación Nacional explica los alcances de la Ley 21.663

El Coordinador Nacional, Daniel Álvarez, y la asesora jurídica y legislativa, Michelle Bordachar, fueron invitados a distintas instancias de conversación para dar a conocer las implicancias que tendrá la nueva Ley Marco de Ciberseguridad. *(**La nota completa, aquí:** https://ciberseguridad.gob.cl/noticias/equipo-de-la-coordinacion-nacional-explica-los-alcances-de-la-ley-21663/)*.

Michelle Bordachar, asesora jurídica y legislativa de la Coordinación, participó en el programa Sesiones de Transformadores de La Tercera. En esta instancia, explicó en detalle sobre los objetivos de la agencia, los Operadores de Importancia Vital, el reporte de incidentes, las multas, el estado de avance de la Ley de Protección de Datos, entre otros temas.

Por su parte, el Coordinador Nacional de Ciberseguridad, Daniel Álvarez Valenzuela fue invitado al Encuentro ODD (Objetivos de Desarrollo Digital) que organiza la Fundación País Digital. En la ocasión, presentó el proceso de implementación de la Ley Marco de Ciberseguridad, en qué consisten sus reglamentos y las facultades que tendrá la Agencia Nacional de Ciberseguridad (ANCI). Participó más tarde en la sesión VTF Day del grupo de coordinación de ciberseguridad de la Asociación de Bancos (ABIF), con el objetivo de explicar los alcances e implicancias de la Ley Marco para el sector financiero.

5. 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 que los sitios web a los que se ingrese sean los oficiales.

5. 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.

- Claudio Andres Obeid Alarcon
- Maria Jose Fuentes
- Kendall Aurelio Davila Reyes
- Victor Cofré
- Diego Bardalez Plaza

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.04.26 17:24:18 -04'00'