CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 212

semana del 21 al 27 de julio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

13

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

22

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

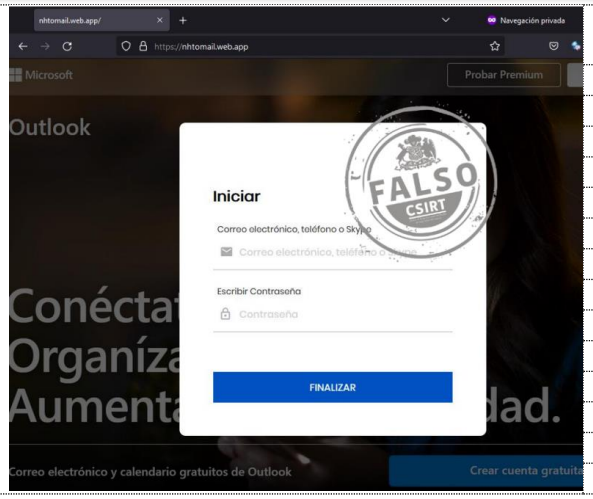
255

Las mitigaciones son útiles en productos de Oracle, Apple, Adobe, Google y MikroTik.

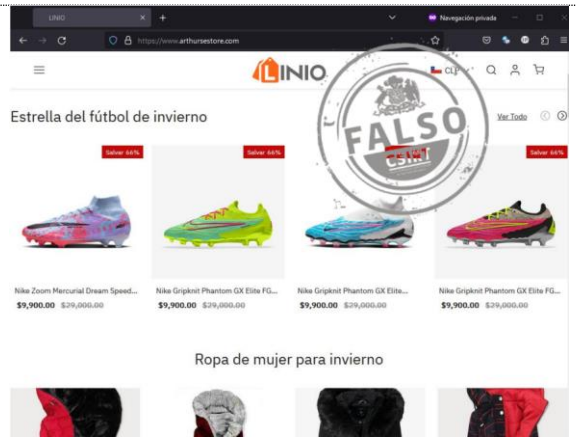
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

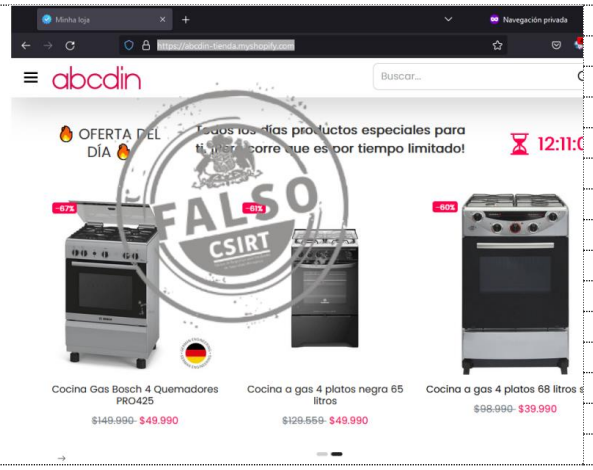
1. Sitios fraudulentos



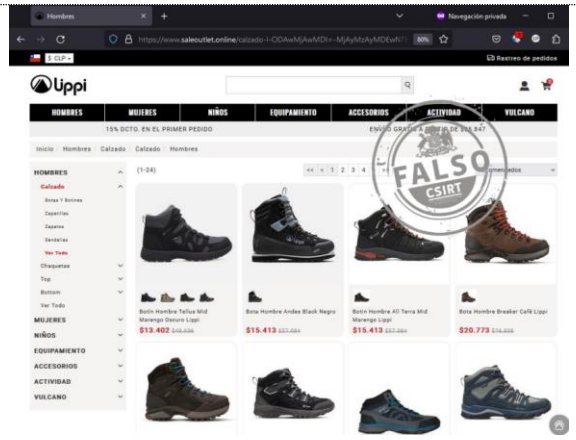
CSIRT alerta de nueva página fraudulenta que suplanta inicio de sesión en Microsoft Outlook	
Alerta de seguridad cibernética	8FFR23-01469-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://nhtomail.web[.]app/	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01469-01/	



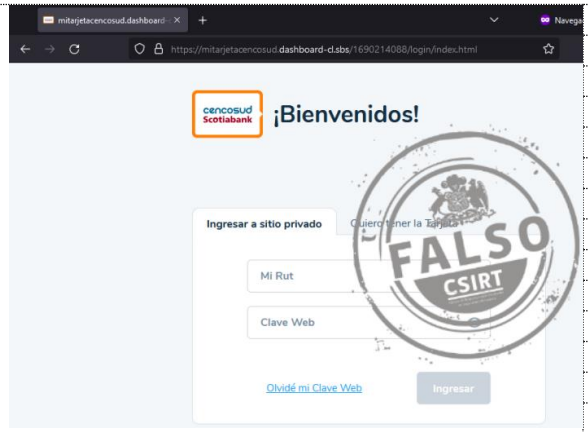
CSIRT alerta de nuevo sitio fraudulento que suplanta a Linio	
Alerta de seguridad cibernética	8FFR23-01470-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.arthursestore[.]com/	
Dirección IP	
[75.2.103.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01470-01/	



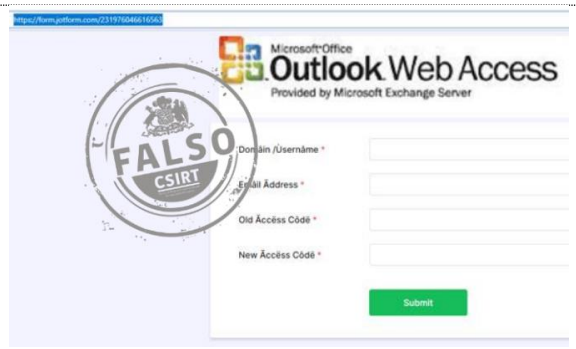
CSIRT alerta de nueva página fraudulenta que suplanta a ABCDin	
Alerta de seguridad cibernética	8FFR23-01471-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://abcdin-tienda.myshopify[.]com/	
Dirección IP	
N/A	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01471-01/	



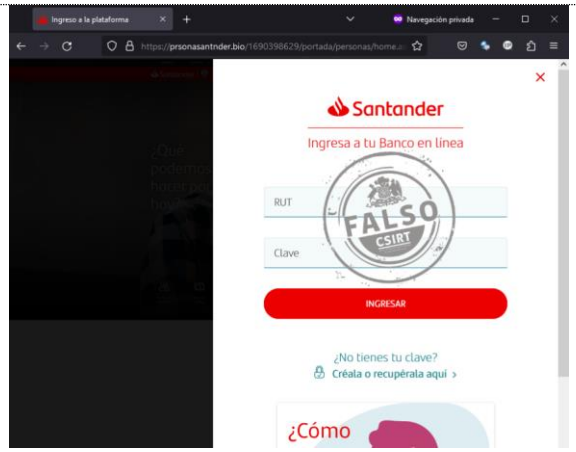
CSIRT alerta de una nueva página fraudulenta que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01472-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://lupioutdoor.mystrikingly[.]com/ https://www.saleoutlet[.]online	
Dirección IP	
[199.21.150.20]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01472-01/	



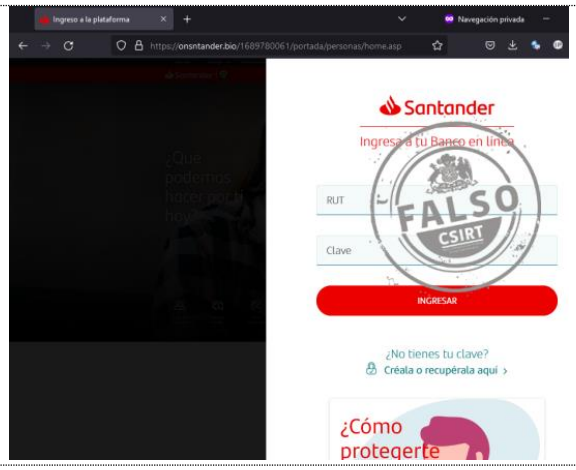
CSIRT alerta de nuevo sitio fraudulento que suplanta a Cencosud Scotiabank	
Alerta de seguridad cibernética	8FFR23-01473-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://mitarjetacencosud.dashboard-cl[.]sbs/1690214088/login/index.html	
Dirección IP	
[104.21.7.81]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01473-01/	



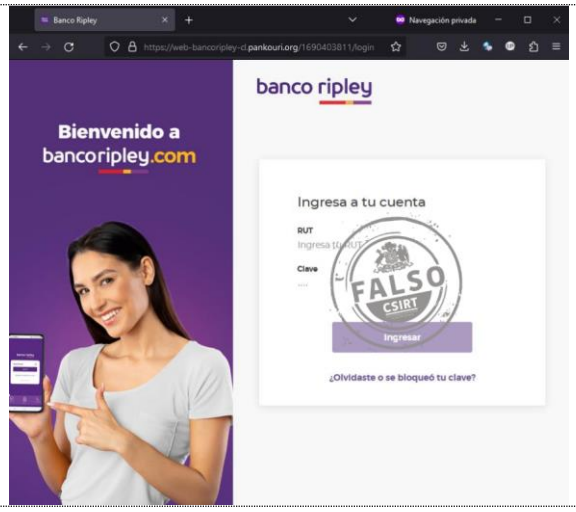
CSIRT alerta de nuevo sitio fraudulento que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR23-01474-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 julio, 2023
Última revisión	26 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://form.jotform[.]com/231976046616563	
Dirección IP	
N/A	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01474-01/	



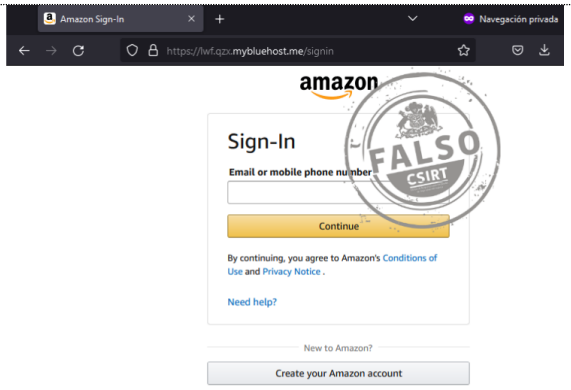
CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01475-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 julio, 2023
Última revisión	27 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://prsonasantnder[.]bio/1690398629/portada/personas/home.asp	
Dirección IP	
[138.128.182.106]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01475-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FFR23-01476-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 julio, 2023
Última revisión	27 julio, 2023
Indicadores de compromiso	
URL sitio falso	
http://yuamflihouse[.]com/1690399065/portada/personas/home.asp	
Dirección IP	
[138.128.182.106]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01476-01/	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FFR23-01477-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 julio, 2023
Última revisión	27 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://web-bancoripley-cl.pankouri[.]org/1690403811/login	
Dirección IP	
[192.185.114.103]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01477-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Amazon	
Alerta de seguridad cibernética	8FFR23-01478-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 julio, 2023
Última revisión	27 julio, 2023
Indicadores de compromiso	
URL sitio falso	
https://lwf.qzx.mybluehost[.]me/signin	
Dirección IP	
[162.215.133.231]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01478-01/	

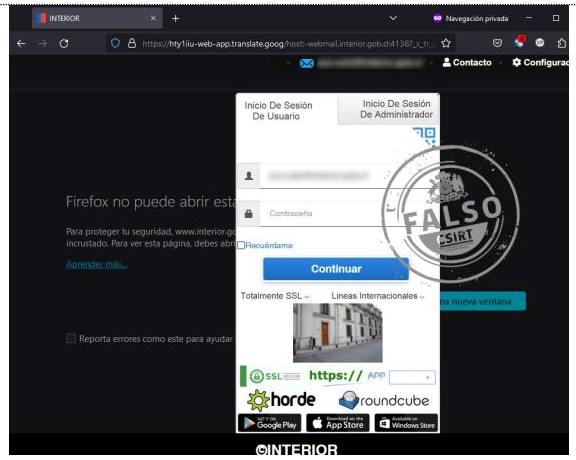
2. Phishing

CSIRT alerta de nueva campaña de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH23-00858-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023
URL sitio falso	
https://firebasestorage.googleapis.com/v0/b/ssssss-f1c45.appspot.com/o/index.html?alt=media&token=06c585b1-eaf3-41bb-aa62-8de7b951d893	
Dirección IP	
N/D	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00858-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a Banco Itaú	
Alerta de seguridad cibernética	8FPH23-00859-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 julio, 2023
Última revisión	25 julio, 2023
Indicadores de compromiso	
URL redirección	
http://ec2-52-67-192-115.sa-east-1.compute.amazonaws[.]com/?hash=bXJvc3NlbGRAaW50ZXJpb3IuZ292LmNs	
URL sitio falso	
https://itau.beneficios-puntos-iupp[.]com/portal/	
Dirección IP sitio falso	
[104.21.13.94]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00859-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00860-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 julio, 2023
Última revisión	25 julio, 2023
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3omdStp	
URL sitio falso	

	https://plazo-banestado.web[.]app/?source=true&kZf1T90oajWmFiEKbcYp5GxC7d6gtDJAN8yQHuvSPq34wXOLlRsMreBlVhnUz2
	Dirección IP sitio falso
	[199.36.158.100]
	Enlace para revisar IoC:
	https://www.csirt.gob.cl/alertas/8fph23-00860-01/



CSIRT alerta de nueva campaña de phishing que suplanta inicio de sesión de email	
Alerta de seguridad cibernética	8FPH23-00861-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 julio, 2023
Última revisión	26 julio, 2023
Indicadores de compromiso	
URL redirección	
https://bql0epapf-xn--luuaryqv-xn—-c1ac4bxc-xn—-p1ai.translate.goog/6ruocAit/0PIl7/e8Pyg?YzI5akxXTnphWEowUUdsdWRHVnlhVzl5TG1kdllpNWpiQT09OjBZclE2+&_x_tr_sch=http&_x_tr_sl=CFEFhLRr&_x_tr_tl=txSzTXAb	
URL sitio falso	
https://hty1iiu-web-app.translate[.]goog/host:-web.interior.gob.cl:0264?_x_tr_sl=wsvfGdH&_x_tr_tl=XDXWjXGI&_x_tr_hist=true	
Dirección IP sitio falso	
[74.125.201.132]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00861-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00862-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 julio, 2023
Última revisión	26 julio, 2023
Indicadores de compromiso	
URL redirección	
https://avengerpatitos[.]com/activacion/cuenta-ezez/	
URL sitio falso	
https://pluscontrolpanel[.]com/1690381385/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[98.142.108.122]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00862-01/	

	CSIRT alerta ante nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00863-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 julio, 2023
Última revisión	27 julio, 2023
Indicadores de compromiso	
URL redirección	
https://avengerpatitos[.]com/activacion/cuenta-ezez/	
URL sitio falso	
https://xank[.]cf/1690465690/imagenes/_personas/home/default.asp	
Dirección IP sitio falso	
[162.240.110.92]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00863-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades del Oracle Critical Patch Update Advisory para julio 2023	
Alerta de seguridad cibernética	9VSA23-00868-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 julio, 2023
Última revisión	24 julio, 2023

CVE

CVE-2018-1282	CVE-2022-3479	CVE-2023-22012
CVE-2018-25032	CVE-2022-36033	CVE-2023-22013
CVE-2019-0227	CVE-2022-36944	CVE-2023-22014
CVE-2019-10086	CVE-2022-37434	CVE-2023-22016
CVE-2019-13990	CVE-2022-37865	CVE-2023-22017
CVE-2019-17531	CVE-2022-40150	CVE-2023-22018
CVE-2020-10735	CVE-2022-40152	CVE-2023-22020
CVE-2020-11988	CVE-2022-40897	CVE-2023-22021
CVE-2020-13936	CVE-2022-41853	CVE-2023-22022
CVE-2020-13956	CVE-2022-41881	CVE-2023-22023
CVE-2020-17521	CVE-2022-41915	CVE-2023-22027
CVE-2020-35168	CVE-2022-41966	CVE-2023-22031
CVE-2020-35169	CVE-2022-42003	CVE-2023-22033
CVE-2020-36518	CVE-2022-42004	CVE-2023-22034
CVE-2020-7760	CVE-2022-42890	CVE-2023-22035
CVE-2020-8908	CVE-2022-42898	CVE-2023-22036
CVE-2021-22569	CVE-2022-42920	CVE-2023-22037
CVE-2021-23926	CVE-2022-43548	CVE-2023-22038
CVE-2021-24112	CVE-2022-43680	CVE-2023-22039
CVE-2021-25220	CVE-2022-4450	CVE-2023-22040
CVE-2021-26117	CVE-2022-45047	CVE-2023-22041
CVE-2021-28168	CVE-2022-45061	CVE-2023-22042
CVE-2021-29425	CVE-2022-45143	CVE-2023-22043
CVE-2021-33813	CVE-2022-45199	CVE-2023-22044
CVE-2021-34429	CVE-2022-45688	CVE-2023-22045
CVE-2021-36090	CVE-2022-45693	CVE-2023-22046
CVE-2021-36374	CVE-2022-45787	CVE-2023-22047
CVE-2021-37533	CVE-2022-46153	CVE-2023-22048
CVE-2021-40528	CVE-2022-46364	CVE-2023-22049
CVE-2021-40690	CVE-2022-48285	CVE-2023-22050
CVE-2021-4104	CVE-2022-4899	CVE-2023-22051
CVE-2021-41183	CVE-2023-0215	CVE-2023-22052
CVE-2021-41184	CVE-2023-0286	CVE-2023-22053
CVE-2021-42575	CVE-2023-0361	CVE-2023-22054
CVE-2021-43113	CVE-2023-0464	CVE-2023-22055
CVE-2021-43859	CVE-2023-0767	CVE-2023-22056
CVE-2021-46877	CVE-2023-1370	CVE-2023-22057
CVE-2022-1122	CVE-2023-1436	CVE-2023-22058
CVE-2022-1471	CVE-2023-1999	CVE-2023-22060
CVE-2022-2048	CVE-2023-20860	CVE-2023-22061
CVE-2022-22950	CVE-2023-20861	CVE-2023-22062
CVE-2022-22971	CVE-2023-20862	CVE-2023-22809

CVE-2022-23305	CVE-2023-20863	CVE-2023-22899
CVE-2022-23437	CVE-2023-20873	CVE-2023-23914
CVE-2022-23491	CVE-2023-21830	CVE-2023-23931
CVE-2022-24409	CVE-2023-21949	CVE-2023-24998
CVE-2022-24891	CVE-2023-21950	CVE-2023-25193
CVE-2022-25147	CVE-2023-21961	CVE-2023-25194
CVE-2022-25647	CVE-2023-21971	CVE-2023-25690
CVE-2022-27404	CVE-2023-21974	CVE-2023-26049
CVE-2022-29361	CVE-2023-21975	CVE-2023-26119
CVE-2022-29546	CVE-2023-21983	CVE-2023-2650
CVE-2022-2963	CVE-2023-21994	CVE-2023-27901
CVE-2022-31129	CVE-2023-22004	CVE-2023-28439
CVE-2022-31160	CVE-2023-22005	CVE-2023-28484
CVE-2022-31197	CVE-2023-22006	CVE-2023-28708
CVE-2022-31692	CVE-2023-22007	CVE-2023-28709
CVE-2022-3171	CVE-2023-22008	CVE-2023-28856
CVE-2022-31777	CVE-2023-22009	CVE-2023-29007
CVE-2022-33879	CVE-2023-22010	CVE-2023-30535
CVE-2022-33980	CVE-2023-22011	CVE-2023-30861

Fabricante

Oracle

Productos afectados

Oracle Communications Billing and Revenue Management 12.0.0.4.0-12.0.0.8.0
Oracle Communications Convergence 3.0.3.2
Oracle Communications Messaging Server 8.1.0.21.0
Oracle Communications Unified Assurance 5.5.0-5.5.17, 6.0.0-6.0.2
Oracle Communications Unified Inventory Management 7.4.1, 7.4.2
Oracle Communications Diameter Signaling Router 8.6.0.0
Oracle Communications Network Analytics Data Director 23.1.0
Oracle Application Testing Suite 13.3.0.1
Oracle Enterprise Manager Ops Center 12.4.0.0
Oracle Banking Corporate Lending 14.0-14.3, 14.5-14.7
Oracle BAM (Business Activity Monitoring) 12.2.1.4.0
Oracle Middleware Common Libraries and Tools 12.2.1.4.0
Oracle WebCenter Content 12.2.1.4.0
Oracle WebLogic Server 12.2.1.4.0, 14.1.1.0.0
Oracle Business Intelligence Enterprise Edition 6.4.0.0.0
Oracle Business Intelligence Enterprise Edition 12.2.1.4.0
Oracle Hyperion Data Relationship Management 11.2.13.0.000
Oracle AutoVue 21.0.2.0-21.0.2.7
Oracle Communications Billing and Revenue Management 12.0.0.4.0-12.0.0.7.0
Oracle HTTP Server 12.2.1.4.0
Oracle SOA Suite 12.2.1.4.0
Oracle Business Intelligence Enterprise Edition 6.4.0.0.0, 7.0.0.0.0, 12.2.1.4.0
MySQL Enterprise Monitor 8.0.34 and prior
Application Express Customers Plugin Application Express Customers Plugin: 18.2-22.2
Application Express Team Calendar Plugin Application Express Team Calendar Plugin: 18.2-22.1
Oracle Communications BRM – Elastic Charging Engine 12.0.0.4.0-12.0.0.8.0
Oracle Communications Cloud Native Core Binding Support Function 22.4.0, 23.1.0
Oracle Banking APIs 21.1.0.0.0, 22.1.0.0.0, 22.2.0.0.0
BI Publisher 7.0.0.0.0
Oracle Hyperion Financial Reporting 11.2.13.0.000

	PeopleSoft Enterprise PeopleTools 8.59, 8.60 Oracle Business Intelligence Enterprise Edition 6.4.0.0.0, 7.0.0.0.0 Oracle TimesTen In-Memory Database 22.1.1.1.0-22.1.1.6.0 JD Edwards EnterpriseOne Tools Prior to 9.2.7.3 Oracle VM VirtualBox Prior to 6.1.46, Prior to 7.0.10 Oracle Enterprise Data Quality 12.2.1.4.0 Oracle Solaris 11 Oracle Hyperion Workspace 11.2.13.0.000 Oracle Graph Server and Client 21.4.6, 22.4.2, 23.1.0 Oracle Commerce Guided Search 11.3.2 Oracle Commerce Platform 11.3.0, 11.3.1, 11.3.2 Oracle Communications BRM – Elastic Charging Engine 12.0.0.4.0-12.0.0.6.0 Oracle Communications Instant Messaging Server 10.0.1.7.0 Oracle Communications Unified Inventory Management 7.4.0-7.4.2, 7.5.0 Oracle Communications Cloud Native Core Automated Test Suite 23.1.1 Oracle Communications Cloud Native Core Automated Test Suite 22.4.1, 23.1.0 Oracle Communications Cloud Native Core Network Exposure Function 22.4.3, 23.1.2 Oracle Communications Cloud Native Core Network Function Cloud Native Environment 23.1.0 Oracle Communications Cloud Native Core Security Edge Protection Proxy 23.1.2, 22.4.3 Oracle Communications Cloud Native Core Service Communication Proxy 22.4.0, 23.1.0 Oracle Communications Cloud Native Core Unified Data Repository 23.1.1 Oracle Banking Branch 14.5-14.7 Oracle Banking Cash Management 14.7.0.2.0, 14.7.1.0.0 Oracle Banking Trade Finance 14.0-14.3, 14.5-14.7 Oracle Access Manager 12.2.1.4.0 Oracle Identity Manager 12.2.1.4.0 Oracle Service Bus 12.2.1.4.0 MySQL Cluster 8.0.33 and prior Siebel CRM 23.4 and prior Siebel CRM 23.6 and prior Siebel CRM 22.12 and prior Primavera Gateway 18.8.0-18.8.15, 19.12.0-19.12.16, 20.12.0-20.12.11, 21.12.0-21.12.9 Oracle Communications Network Integrity 7.3.6.4 Oracle Communications Order and Service Management 7.4.1 Oracle Communications Pricing Design Center 12.0.0.4.0-12.0.0.7.0 Oracle Communications Cloud Native Core Network Repository Function 23.1.0, 23.2.0 Oracle Communications Cloud Native Core Network Repository Function 23.1.1 Oracle Web Applications Desktop Integrator 12.2.3-12.2.12 Oracle Enterprise Manager for Fusion Middleware 13.5.0.0 Oracle Enterprise Manager for Oracle Database 13.5.0.0 Oracle Data Integrator 12.2.1.4.0 Oracle Mobile Security Suite Prior to 11.1.2.3.1 Oracle Health Sciences Sciences Data Management Workbench 3.1.0.2, 3.1.1.3, 3.2.0.0 Oracle GoldenGate Stream Analytics 19.1.0.0.0-19.1.0.0.7 Oracle Applications Framework 12.2.3-12.3.12 Oracle Scripting 12.2.3-12.2.12 BI Publisher 6.4.0.0.0 JD Edwards EnterpriseOne Tools Prior to 9.2.7.4

	Siebel CRM 23.5 and prior Oracle Hyperion Essbase Administration Services 21.4.3.0.0 Oracle Communications Cloud Native Core Security Edge Protection Proxy 23.1.2 Oracle Java SE Oracle Java SE: 8u371 MySQL Server 5.7.42 and prior, 8.0.33 and prior Application Express Administration Application Express Administration: 18.2-22.2 Oracle Communications Cloud Native Core Console 22.4.2, 23.1.1 Oracle Business Process Management Suite 12.2.1.4.0 Oracle WebLogic Server 14.1.1.0.0 JD Edwards EnterpriseOne Orchestrator Prior to 9.2.7.4 Oracle Agile PLM 9.3.6 Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1 Unified Audit 19.3-19.19, 21.3-21.10 MySQL Server 8.0.33 and prior MySQL Server 8.0.27 and prior MySQL Server 5.7.41 and prior, 8.0.32 and prior Oracle WebLogic Server 14.1.1.0.0, 12.2.1.4.0 Oracle Applications Technology 12.2.3-12.2.12 Oracle Self-Service Human Resources 12.2.3-12.2.12 Oracle Business Intelligence Enterprise Edition 7.0.0.0.0 Advanced Networking Option 19.3-19.19, 21.3-21.10 Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1 Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1 Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 8u371-perf, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1 Oracle Java SE, Oracle GraalVM Enterprise Edition, Oracle GraalVM for JDK Oracle Java SE: 8u371, 8u371-perf, 11.0.19, 17.0.7, 20.0.1; Oracle GraalVM Enterprise Edition: 20.3.10, 21.3.6, 22.3.2; Oracle GraalVM for JDK: 17.0.7, 20.0.1 Java VM 19.3-19.19, 21.3-21.10 Oracle Essbase 21.4.3.0.0
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00868-01/

CSIRT comparte información de vulnerabilidades dadas a conocer por Apple para iOS, iPadOS, macOS y Safari	
Alerta de seguridad cibernética	9VSA23-00869-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 julio, 2023
Última revisión	25 julio, 2023

CVE

CVE-2023-23540	CVE-2023-32443	CVE-2023-38425
CVE-2023-28319	CVE-2023-32734	CVE-2023-38564
CVE-2023-28320	CVE-2023-35983	CVE-2023-38565
CVE-2023-28321	CVE-2023-35993	CVE-2023-38572
CVE-2023-28322	CVE-2023-36854	CVE-2023-38580
CVE-2023-2953	CVE-2023-36862	CVE-2023-38593
CVE-2023-32364	CVE-2023-37450	CVE-2023-38594
CVE-2023-32381	CVE-2023-38133	CVE-2023-38595
CVE-2023-32409	CVE-2023-38136	CVE-2023-38597
CVE-2023-32416	CVE-2023-38258	CVE-2023-38600
CVE-2023-32418	CVE-2023-38259	CVE-2023-38602
CVE-2023-32429	CVE-2023-38261	CVE-2023-38603
CVE-2023-32433	CVE-2023-38410	CVE-2023-38606
CVE-2023-32437	CVE-2023-38421	CVE-2023-38608
CVE-2023-32441	CVE-2023-38424	CVE-2023-38611
CVE-2023-32442		

Fabricante

Apple

Productos afectados

Versiones de iOS anteriores a 15.7.1., iPhone, iPad

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00869-01/

CSIRT comparte información de vulnerabilidades parchadas por Adobe para ColdFusion e InDesign	
Alerta de seguridad cibernética	9VSA23-00870-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 julio, 2023
Última revisión	25 julio, 2023

CVE

CVE-2023-29298
CVE-2023-38203
CVE-2023-38204
CVE-2023-38205
CVE-2023-38206

Fabricante

Adobe

Productos afectados

ColdFusion 2018
ColdFusion 2021

	ColdFusion 2023 Adobe InDesign ID18.3 y anteriores. Adobe InDesign ID17.4.1. y anteriores. **Enlaces para revisar el informe:** https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00870-01/

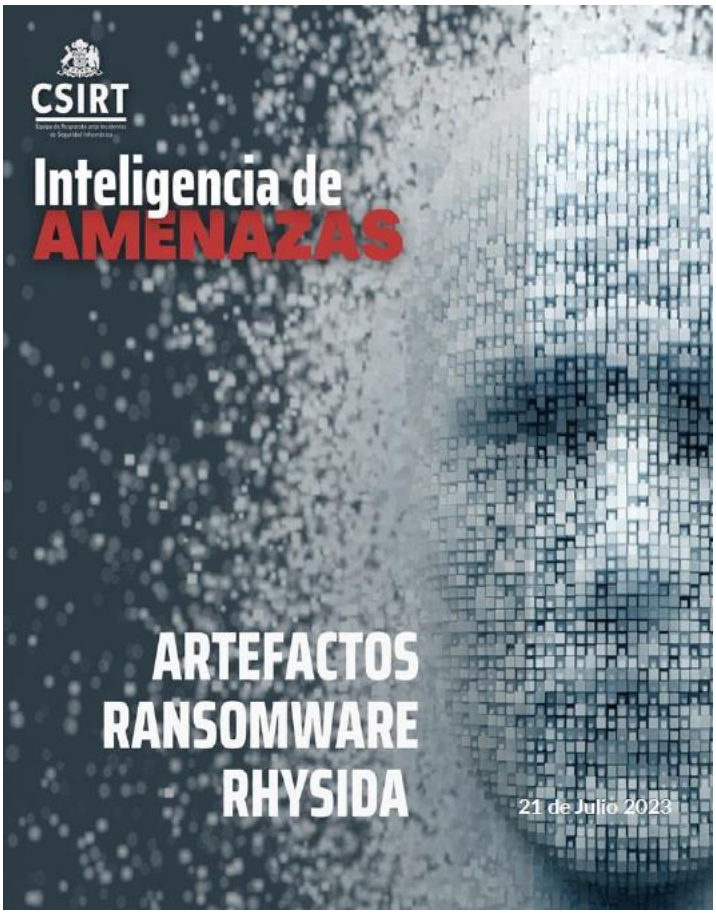
CSIRT comparte vulnerabilidades parchadas en Google Chrome 115		
Alerta de seguridad cibernética	9VSA23-00871-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	25 julio, 2023	
Última revisión	25 julio, 2023	
CVE		
CVE-2023-3727	CVE-2023-3733	CVE-2023-3737
CVE-2023-3728	CVE-2023-3734	CVE-2023-3738
CVE-2023-3730	CVE-2023-3735	CVE-2023-3740
CVE-2023-3732	CVE-2023-3736	
Fabricante		
Google		
Productos afectados		
Google Chrome		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00871-01/		

CSIRT comparte información de vulnerabilidad crítica en MikroTik RouterOS	
Alerta de seguridad cibernética	9VSA23-00872-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 julio, 2023
Última revisión	26 julio, 2023
CVE	
CVE-2023-30799	
Fabricante	
Mikrotik	
Productos afectados	
MikroTik RouterOS stable anteriores a la versión 6.49.7 y long-term hasta la 6.48.6.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00872-01/	

4. Concientización

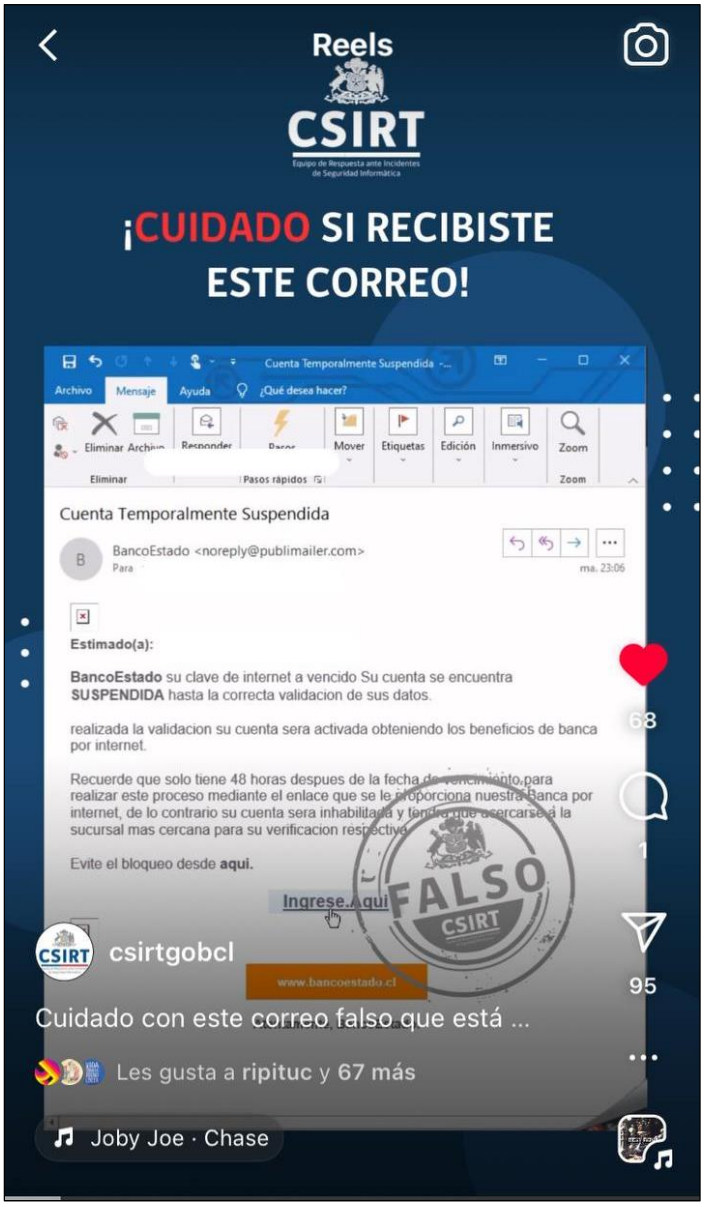
Inteligencia de Amenazas No. 1: Ransomware Rhysida

Desde el CSIRT de Gobierno los invitamos a leer nuestro primer análisis de Inteligencia de Amenazas, hecho sobre lo que nuestros especialistas vieron al estudiar el novedoso ransomware Rhysida. Para acceder al archivo, solo basta con hacer clic aquí: https://www.csirt.gob.cl/media/2023/07/14TCA23-00011-01.pdf



Video contra el phishing

Esta semana, compartimos en nuestro Instagram un reel que enseña en qué poner atención para no caer en una campaña de phishing. Pueden encontrarlo aquí: https://www.instagram.com/reel/CvK7RNXAyp-/?igshid=MzRlODBiNWFlZA.



Ciberdiccionario Volumen 41

En el ciberdiccionario del CSIRT, esta semana les traemos definiciones para clearweb, ataque de diccionario, dominio de nivel superior y ciberataque. ¡Esperamos les sean útiles! Encuentrenlo también aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-41/.

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.

6. 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.

- Nicolás Friz Pereira
- Francisco Flores
- Pablo Ignacio Pizarro Cortinez
- Francisco Alejandro Carrasco Zepeda
- Natán Finol Bencomo
- Mauro Javier Esteban Cabezas González
- Eugenio Escudero Ortúzar
- Diego Salazar
- Washington Maturana
- Omar Díaz
- Natalia Mesa Videla
- Ingrid Junod Alcaíno

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.28 18:18:57 -04'00'