CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 18

SEMANA DEL 30 DE DICIEMBRE DE 2022
AL 5 DE ENERO DE 2023

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

66

Las mitigaciones son útiles en productos de Fortinet, IBM, Google (Android) y Zoho.

IP INFORMADAS

13

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

URL ADVERTIDAS

25

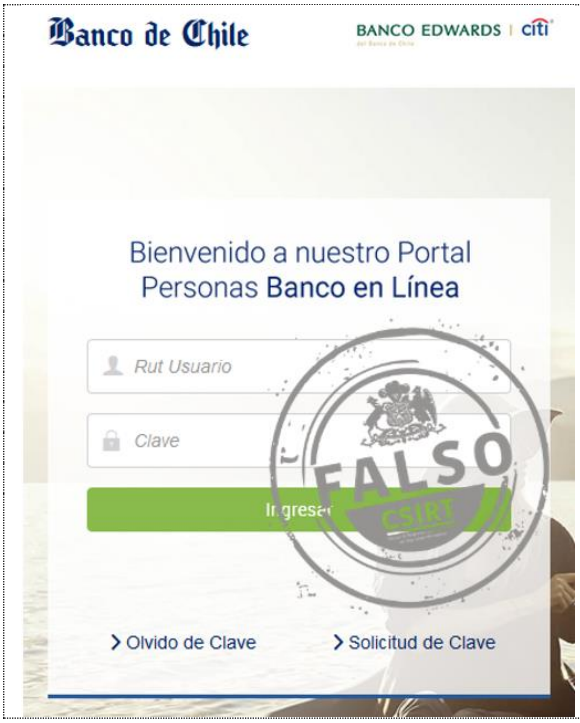
Asociadas a sitios fraudulentos y campañas de phishing y malware

CONTENIDO

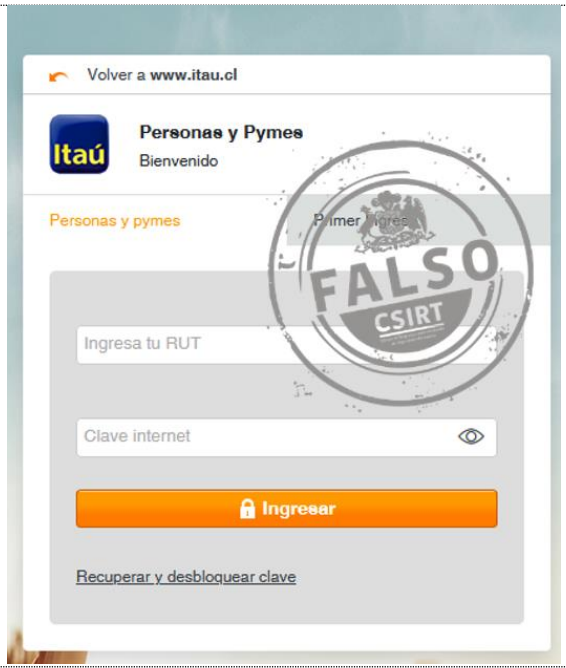
1. Sitios fraudulentos 3
2. Phishing 6
3. Vulnerabilidades 9
4. Concientización 11
5. Recomendaciones y buenas prácticas 12
6. Muro de la Fama 13

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos

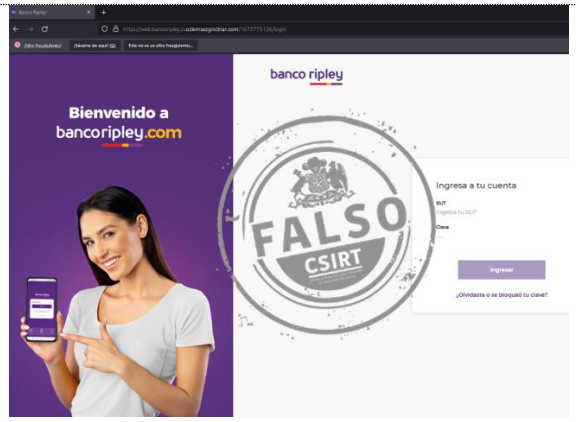


CSIRT alerta de nueva página fraudulenta que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FFR22-01184-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2022
Última revisión	30 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//portal-bancochile.cl.townrealstate[.]com/1672425960/bchile-web/persona/login/index.html/login	
Dirección IP	
[185.146.22.242]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01184-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01184-01.pdf	

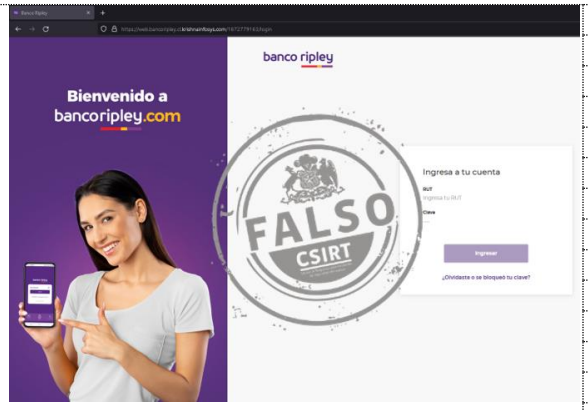


CSIRT alerta de nueva página fraudulenta que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FFR22-01185-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2022
Última revisión	30 de diciembre de 2022
Indicadores de compromiso	
URL sitio falso	
https[:]//wwv.bnnco.ltau.cl.scgfounders[.]com/1672426652/bancochile-web/persona/login/index.html/login	
Dirección IP	
[162.241.169.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01185-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01185-01.pdf	

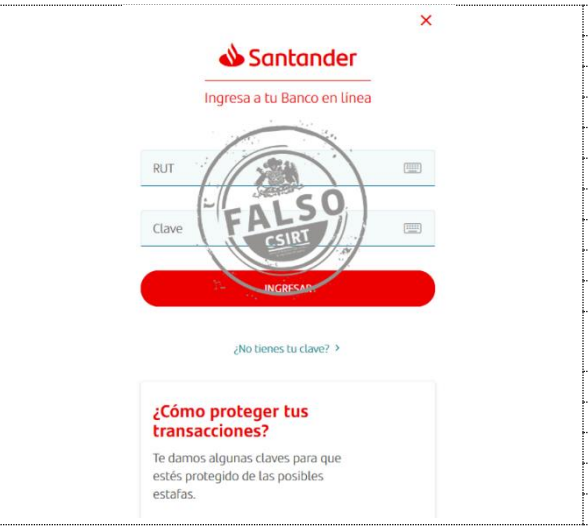
CSIRT alerta de una página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01186-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de enero de 2023
Última revisión	3 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//santanderchile-personas.dmklaws.co[.]ke/1672770309/portada/personas/home.asp	
Dirección IP	
[109.106.250.12]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01186-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01186-01.pdf	



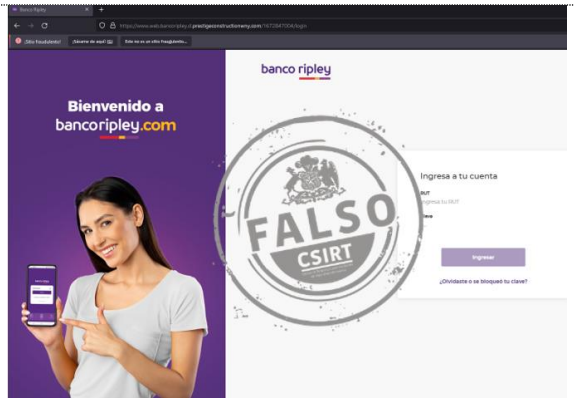
CSIRT alerta de la activación de una página fraudulenta que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR22-01187-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de enero de 2023
Última revisión	3 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//web.bancoripley.cl.ozlemsezgincinar[.]com/1672775136/login	
Dirección IP	
[185.179.27.31]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01187-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01187-01.pdf	



CSIRT alerta de una página fraudulenta que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR22-01188-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//web.bancoripley.cl.krishnainfosys[.]com/1672779163/login	
Dirección IP	
[78.142.63.93]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01188-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01188-01.pdf	

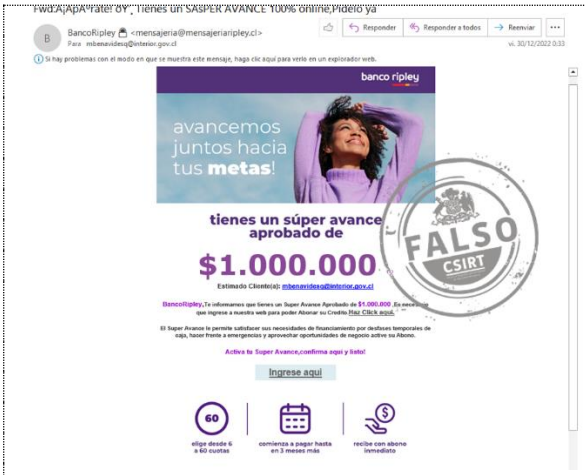


CSIRT alerta ante página fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01189-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//santanderchile-personas.dmklaws.co[.]ke/1672845677/portada/personas/home.asp	
Dirección IP	
[109.106.250.12]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01189-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01189-01.pdf	



CSIRT alerta de página fraudulenta que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR22-01190-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.web.bancoripley.cl.prestigeconstructionwny[.]com/1672847004/login	
Dirección IP	
[192.185.21.172]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01190-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR22-01190-01.pdf	

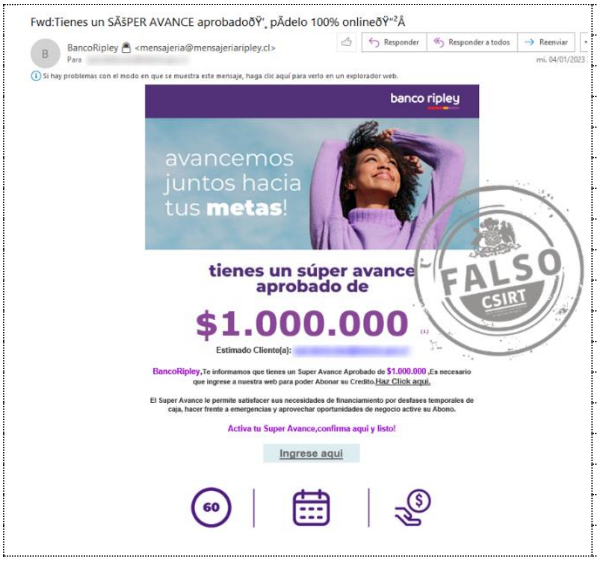
2. Phishing



CSIRT alerta de campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00696-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2022
Última revisión	30 de diciembre de 2022
URL redirección	
https[:]//bit[.]ly/3FWRqvY?l=www.bancoripley.cl https[:]//mpza[.]sk/bancoripley/cuenta-qksa/	
URL sitio falso	
https://web.banc0ripleycl.buckrealty[.]net/1672404123/login	
IP	
[64.91.247.208]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00696-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00696-01.pdf	

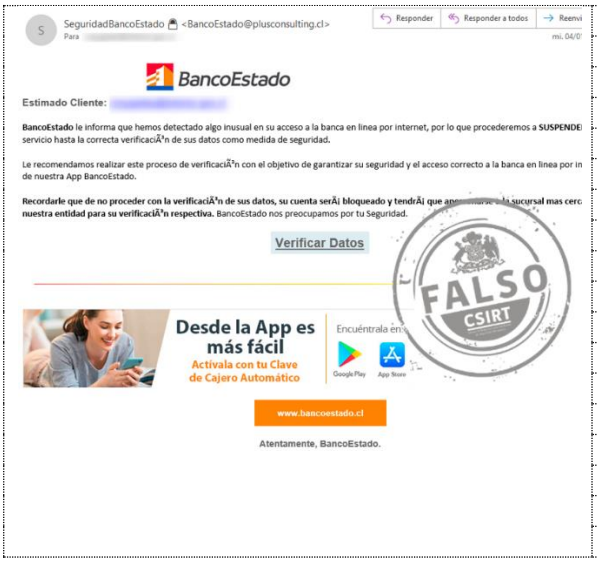
CSIRT alerta de nueva campaña de phishing con sextorsión	
Alerta de seguridad cibernética	8FPH22-00697-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de diciembre de 2022
Última revisión	30 de diciembre de 2022
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00697-01/	
https://www.csirt.gob.cl/media/2022/12/8FPH22-00697-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00698-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	3 de enero de 2023
Última revisión	3 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3Z8OkOn?l=www.bancoripley.cl	
URL sitio falso	
https[:]//web.bancoripley.cl.bluewayeducation[.]in/1672748142/login	
Dirección IP	
[43.225.55.146]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00698-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH22-00698-01.pdf	

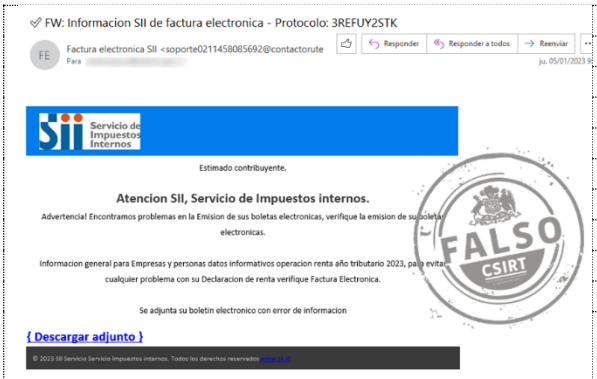


CSIRT alerta de campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00699-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3Qazxyo?l=www.bancoripley.cl	
URL sitio falso	
https[:]//web-bancoripley-cl.wonthaggicaravans.com[.]au/1672836015/login	
Dirección IP	
[203.26.41.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00699-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH22-00699-01.pdf	

CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00700-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-aotq/	
URL sitio falso	
https[:]//smscotito[.]info/1672861250/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.133.17]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00700-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00700-01.pdf	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00701-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//xtraillconver[.]com/activacion/cuenta-hkgr/	
URL sitio falso	
https[:]//nmhpatito[.]info/1672863063/imagenes/_personas/home/default.asp	
Dirección IP	
[162.241.60.24]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00701-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00701-01.pdf	



CSIRT alerta de nueva campaña de phishing con malware, que suplanta al SII	
Alerta de seguridad cibernética	8FPH23-00702-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de enero de 2023
Última revisión	5 de enero de 2023
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00702-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00702-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00703-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de enero de 2023
Última revisión	6 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//web-bancoripley-cl.wonthaggicaravans.com[.]au/1673009665/login	
URL sitio redirección	
https[:]//bit[.]ly/3CruO5Z?l=www.bancoripley.cl	
Dirección IP	
[203.26.41.136]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00703-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00703-01.pdf	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades que afectan a FortiADC y FortiTester	
Alerta de seguridad cibernética	9VSA22-00760-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
CVE	
CVE-2022-39947 CVE-2022-35845	
Fabricantes	
Fortinet	
Productos afectados	
FortiADC versión 7.0.0 a 7.0.2 FortiADC versión 6.2.0 a 6.2.3 FortiADC versión 6.1.0 a 6.1.6 FortiADC versión 6.0.0 a 6.0.4 FortiADC versión 5.4.0 a 5.4.5	FortiTester versión 7.1.0 FortiTester versión 7.0 todas FortiTester versión 4.0.0 a 4.2.0 FortiTester versión 2.3.0 a 3.9.1
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00760-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA22-00760-01.pdf	

CSIRT comparte información sobre vulnerabilidades en actualización de seguridad de Android para enero 2023		
Alerta de seguridad cibernética	9VSA22-00761-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	4 de enero de 2023	
Última revisión	4 de enero de 2023	
CVE		
CVE-2022-20456	CVE-2022-42720	CVE-2022-44437
CVE-2022-20489	CVE-2022-42721	CVE-2022-44438
CVE-2022-20490	CVE-2022-2959	CVE-2022-22088
CVE-2022-20492	CVE-2022-41674	CVE-2022-33255
CVE-2022-20493	CVE-2023-20928	CVE-2021-35097
CVE-2023-20912	CVE-2022-20235	CVE-2021-35113
CVE-2023-20916	CVE-2022-32635	CVE-2021-35134
CVE-2023-20918	CVE-2022-32636	CVE-2022-23960
CVE-2023-20919	CVE-2022-32637	CVE-2022-25725
CVE-2023-20920	CVE-2022-44425	CVE-2022-25746
CVE-2023-20921	CVE-2022-44426	CVE-2022-33252
CVE-2022-20494	CVE-2022-44427	CVE-2022-33253
CVE-2023-20908	CVE-2022-44428	CVE-2022-33266
CVE-2023-20922	CVE-2022-44429	CVE-2022-33274
CVE-2022-20461	CVE-2022-44430	CVE-2022-33276
CVE-2023-20904	CVE-2022-44431	CVE-2022-33283
CVE-2023-20905	CVE-2022-44432	CVE-2022-33284
CVE-2023-20913	CVE-2022-44434	CVE-2022-33285

	CVE-2023-20915 CVE-2022-42719	CVE-2022-44435 CVE-2022-44436	CVE-2022-33286
	Fabricantes		
	Google		
	Productos afectados		
	Android, todas las versiones.		
	Enlaces para revisar el informe:		
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00761-01/		
	https://www.csirt.gob.cl/media/2023/01/9VSA23-00761-01.pdf		

CSIRT comparte información de vulnerabilidades parchadas para IBM Cloud Pak for Business Automation	
Alerta de seguridad cibernética	9VSA23-00762-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	5 de enero de 2023
Última revisión	5 de enero de 2023
CVE	
CVE-2017-10355 CVE-2022-42920	CVE-2022-42435 CVE-2022-2047
Fabricantes	
IBM	
Productos afectados	
IBM Cloud Pak for Business Automation anteriores a 21.0.3-IF016 y 22.0.1-IF006, las que corrigen las presentes vulnerabilidades.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00762-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00762-01.pdf	

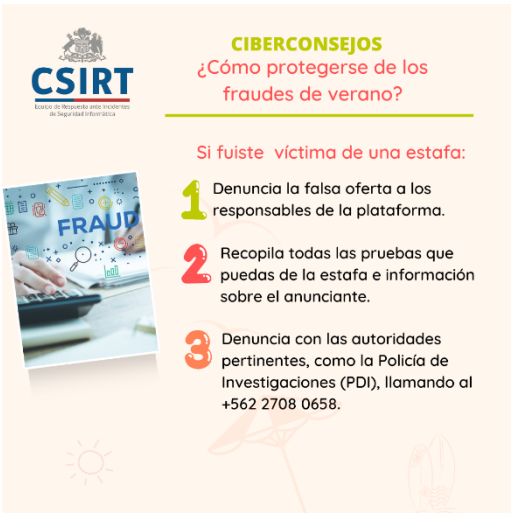
CSIRT comparte vulnerabilidades informadas para distintos productos de Zoho	
Alerta de seguridad cibernética	9VSA23-00763-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	4 de enero de 2023
Última revisión	4 de enero de 2023
CVE	
CVE-2022-47523	
Fabricantes	
Fortinet	
Productos afectados	
Access Manager Plus 12200 y anteriores. PAM360 5800 y anteriores, Password Manager Pro 4308 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00763-01/	
https://www.csirt.gob.cl/media/2023/01/9VSA23-00763-01.pdf	

4. Concientización

Ciberconsejos: ¿Cómo protegerse de los fraudes de verano?

Cada vez son más las personas que arriendan alguna propiedad para sus vacaciones de verano a través de un sitio web. Sin embargo, así como incrementa esta tendencia también aparecen los avisos falsos que buscan obtener un beneficio económico.

Para evitar caer en este tipo de estafas, el CSIRT de Gobierno entregó esta semana las siguientes recomendaciones, disponibles también en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-estafas-verano/



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.

- Cristián Figueroa Valenzuela
- Rodrigo Machado Villegas
- Gerardo Andrés Hernández Rodríguez
- David Soto
- Christopher Provoste Álvarez
- Juan Pablo Andrés Garrido Lara
- Rodrigo Andrés Cáceres Valdés.