



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 242

semana del 16 al 22 de febrero de 2024

LA SEMANA EN CIFRAS

IP INFORMADAS

5

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

7

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

19

Las mitigaciones son útiles en productos de Mozilla, Joomla y VMware



CONTENIDO

1. Phishing	3
2. Sitios fraudulentos.....	5
3. Vulnerabilidades.....	6
5. Noticias y concientización.....	8
6. Recomendaciones y buenas prácticas	9
7. Muro de la Fama	10

1. Phishing



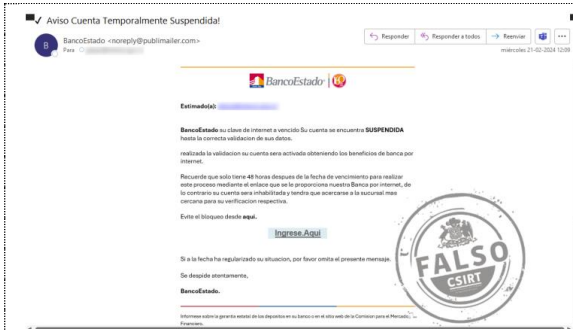
CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH24-00929-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 febrero, 2024
Última revisión	16 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://wwwbanc0chil3com.shahanshasports[.]com/1708090726/imagenes/_per_sonas/home/default.asp	
URL de redirección	
https://maximocontaval[.]com/activacion/cuenta-kaoi/	
Dirección IP sitio falso	
[162.0.220.139]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00929-01/	



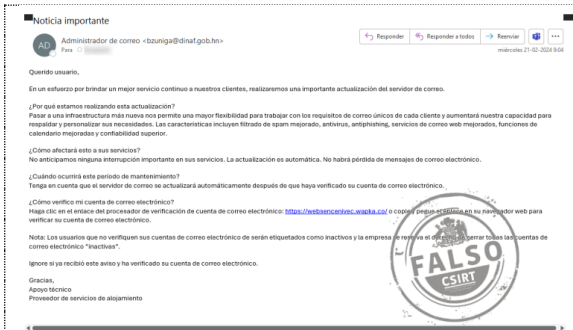
CSIRT alerta de nueva campaña de phishing en falso aviso de cambio de contraseña

Alerta de seguridad cibernética	8FPH24-00930-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 febrero, 2024
Última revisión	16 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://share.formbold[.]com/6M7G7	
Dirección IP sitio falso	
[172.67.160.57]	
Enlace para revisar IoC:	
https://csirt.gob.cl/alertas/8fph24-00930-01/	



CSIRT alerta de campaña de phishing que suplanta a BancoEstado

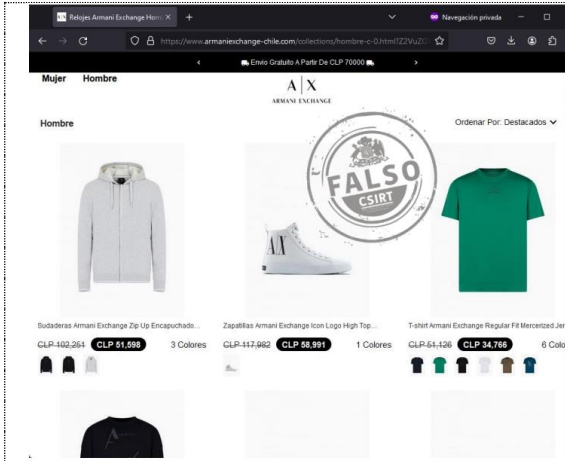
Alerta de seguridad cibernética	8FPH24-00931-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 febrero, 2024
Última revisión	21 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://wwwbancoestadocl.theaerie[.]ca/1708528751/imagenes/_personas/home/default.asp	
URL redirección	
https://underconcentral[.]com/activacion/cuenta-qdur/	
Dirección IP sitio falso	
[192.185.138.178]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8fph24-00931-01/	



CSIRT alerta de campaña de phishing que suplanta a un servidor de correo

Alerta de seguridad cibernética	8FPH24-00932-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 febrero, 2024
Última revisión	21 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://websencenivec.wapka[.]co/	
Dirección IP sitio falso	
[181.210.30.114]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8fph24-00932-01/	

2. Sitios fraudulentos



CSIRT advierte nuevo sitio falso que suplanta a Armani Exchange

Alerta de seguridad cibernética	8FFR23-01645-01
Clase de alerta	Fraude
Tipo de incidente	Fraude
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 febrero, 2024
Última revisión	21 febrero, 2024
Indicadores de compromiso	
URL del sitio falso	
https://www.armaniexchange-chile[.]com	
Dirección IP sitio falso	
[196.196.192.140]	
Enlace para revisar loC:	
https://csirt.gob.cl/alertas/8ffr24-01645-01/	

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

3. Vulnerabilidades



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA24-00977-01
 CSIRT comparte información de vulnerabilidades en Firefox 123

PARA REGISTRAR | 1510
 UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte vulnerabilidades en Firefox 123

Alerta de seguridad cibernética	9VSA24-00977-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 febrero, 2024
Última revisión	21 febrero, 2024

CVE

CVE-2024-1546	CVE-2024-1549	CVE-2024-1556
CVE-2024-1547	CVE-2024-1550	CVE-2024-1552
CVE-2024-1554	CVE-2024-1551	CVE-2024-1553
CVE-2024-1548	CVE-2024-1555	CVE-2024-1557

Fabricante

Mozilla

Productos afectados

Firefox 123, Firefox ESR 115.8 y Thunderbird 115.8.

Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa24-00977-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA24-00978-01
 CSIRT comparte información de vulnerabilidades en VMware

PARA REGISTRAR | 1510
 UN INCIDENTE | www.csirt.gob.cl

CSIRT
 Equipo de Respuesta ante Incidentes de Seguridad Informática

CSIRT comparte información de vulnerabilidades en VMware

Alerta de seguridad cibernética	9VSA24-00978-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 febrero, 2024
Última revisión	21 febrero, 2024

CVE

CVE-2024-22245
CVE-2024-22250

Fabricante

VMware

Productos afectados

Complemento de autenticación mejorada (EAP) de VMware.

Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa24-00978-01/>

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>



CSIRT comparte información de vulnerabilidades en Joomla

Alerta de seguridad cibernética	9VSA24-00979-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 febrero, 2024
Última revisión	22 febrero, 2024

CVE

CVE-2024-21722
CVE-2024-21723
CVE-2024-21724
CVE-2024-21725
CVE-2024-21726

Fabricante

Joomla





Productos afectados

Series 5.x y 4.x de Joomla.

Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa24-00979-01/>

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

5. Noticias y concientización

Ciberconsejos | Cuida tus hijos en redes sociales

Compartir las fotografías de tus hijos en redes sociales puede ser inofensivo, sin embargo, existen algunos riesgos asociados, entre ellos, estafas o suplantación de identidad y uso indebido de sus fotografías.

Ver más: <https://csirt.gob.cl/recomendaciones/ciberconsejos-cuida-tus-hijos-en-redes-sociales/>



En redes sociales, preocúpate que tus hijos:

- Nunca compartan datos personales como nombres, dirección u otros.
- Tengan su perfil en modo privado y acepten solo a personas conocidas.
- No hablen con desconocidos. Explícales los riesgos.



¡Cuidado con el sharenting!

Es la práctica que tienen algunos padres de publicar las fotos de sus hijos en redes sociales.

Cuida la privacidad de los menores:

- Desactiva la ubicación y geolocalización.
- Nunca publiques fotografías de los niños sin ropa.
- Deshabilita la opción "compartir" tus fotografías.
- Evita publicar nombres, fecha de nacimiento, edad, etc.

CONTACTO Y REDES SOCIALES CSIRT

6. 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.

CONTACTO Y REDES SOCIALES CSIRT

7. 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.

- Sebastián Larra
- Rossana Robles
- Francisco Flores
- Francisco Espinoza

CONTACTO Y REDES SOCIALES CSIRT