



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 221

semana del 22 al 28 de septiembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

3

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

3

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

18

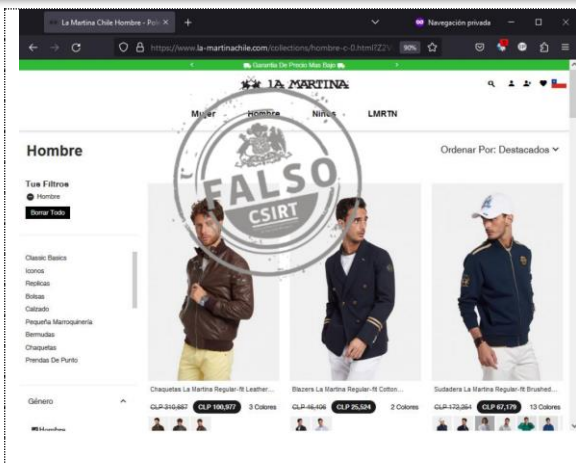
Las mitigaciones son útiles en productos de Apple, Google, BIND, libwebp y Mozilla.



CONTENIDO

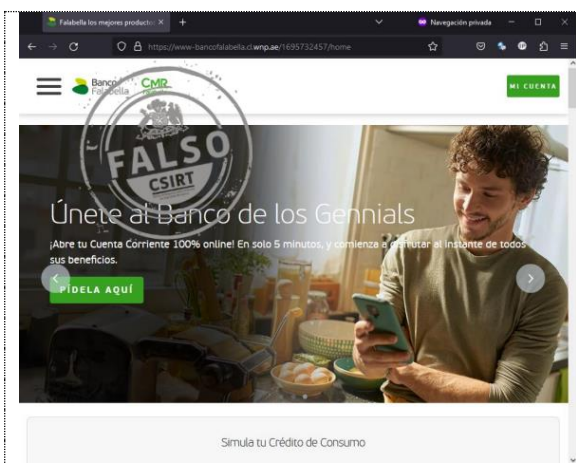
1.	Sitios fraudulentos	3
2.	Vulnerabilidades	4
3.	Noticias y concientización	7
4.	Recomendaciones y buenas prácticas	10
5.	Muro de la Fama	11

1. Sitios fraudulentos



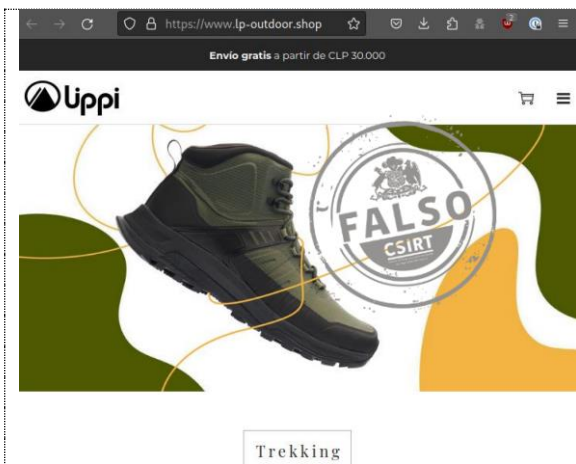
CSIRT alerta de nueva página fraudulenta que suplanta a La Martina

Alerta de seguridad cibernética	8FFR23-01533-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 septiembre, 2023
Última revisión	26 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	https://www.la-martinachile[.]com
IP del sitio falso	[196.196.223.4]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01533-01/



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Falabella

Alerta de seguridad cibernética	8FFR23-01534-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 septiembre, 2023
Última revisión	26 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	https://www-bancofalabella[.]cl.wnp.ae/1695732457/home
IP del sitio falso	[109.70.148.54]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01534-01/



CSIRT alerta de nueva página fraudulenta que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01535-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 septiembre, 2023
Última revisión	28 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	https://www.lp-outdoor[.]shop/
IP del sitio falso	[109.70.148.54]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01535-01/

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>

2. Vulnerabilidades



CSIRT informa de parches preparados por Apple para nuevas vulnerabilidades de día cero

Alerta de seguridad cibernética	9VSA23-00906-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 septiembre, 2023
Última revisión	22 septiembre, 2023

CVE

CVE-2023-41991
CVE-2023-41992
CVE-2023-41993

Fabricante

Apple

Productos afectados

Actualizaciones iOS 16.7 y iPadOS 16.7: Disponible para iPhone 8 y posteriores, iPad Pro, iPad Air 3ra generación y posteriores, iPad 5ta generación y posteriores, iPad mini 5ta generación y posteriores.

Actualizaciones iOS 17.0.1 y iPadOS 17.0.1: Disponibles iPhone XS y posteriores, iPad Pro 12.9 pulgadas 2da generación y posteriores, iPad Pro 10.5 pulgadas, iPad Pro 11 pulgadas 1ra generación y posteriores, iPad Air 3ra generación y posteriores, iPad 6ta generación y posteriores, iPad mini 5ta generación y posteriores.

macOS Monterey

macOS Ventura

watchOS 9.6.3 y watchOS 10.0.1 disponible para Apple Watch serie 4 y posteriores.

Safari 16.6.1 disponible para macOS Big Sur y Monterey.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00906-01/>

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>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00907-01
CSIRT informa de vulnerabilidades de alto riesgo en BIND. Parches disponibles

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



CSIRT informa de dos vulnerabilidades de alto riesgo en BIND, para las cuales existen parches disponibles

Alerta de seguridad cibernética	9VSA23-00907-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 septiembre, 2023
Última revisión	22 septiembre, 2023

CVE

CVE-2023-3341
 CVE-2023-4236

Fabricante

Internet Systems Consortium

Productos afectados

BIND 9
 9.2.0 -> 9.16.43
 9.18.0 -> 9.18.18
 9.19.0 -> 9.19.16

BIND Supported Preview Edition

9.9.3-S1 -> 9.16.43-S1
 9.18.0-S1 -> 9.18.18-S1

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00907-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00908-01
CSIRT informa de vulnerabilidad crítica en libwebp, parchada en Google Chrome

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



CSIRT comparte información de vulnerabilidad crítica en libwebp, parchada para Google Chrome

Alerta de seguridad cibernética	9VSA23-00908-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 septiembre, 2023
Última revisión	27 septiembre, 2023

CVE

CVE-2023-5129

Fabricante

Google

Productos afectados

Google Chrome anteriores a 116.0.5845.187.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00908-01/>

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>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00909-01
CSIRT informa vulnerabilidad de día cero parchada en actualización Google Chrome

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



CSIRT informa de nueva vulnerabilidad de día cero que afecta a Google Chrome, parchada en su más reciente actualización

Alerta de seguridad cibernética	9VSA23-00909-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 septiembre, 2023
Última revisión	28 septiembre, 2023

CVE

CVE-2023-5217
 CVE-2023-5186
 CVE-2023-5187

Fabricante

Google

Productos afectados

Google Chrome

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00909-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00910-01
CSIRT informa vulnerabilidades parchadas en productos de Mozilla como Firefox

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



CSIRT comparte información de nuevas vulnerabilidades que fueron parchadas en Firefox, Firefox ESR y Thunderbird

Alerta de seguridad cibernética	9VSA23-00910-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 septiembre, 2023
Última revisión	28 septiembre, 2023

CVE

CVE-2023-5168
 CVE-2023-5169
 CVE-2023-5170
 CVE-2023-5171
 CVE-2023-5172
 CVE-2023-5173
 CVE-2023-5174
 CVE-2023-5175
 CVE-2023-5176

Fabricante

Mozilla

Productos afectados

Mozilla Firefox, Firefox ESR y Thunderbird.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00910-01/>

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. Noticias y concientización

CSIRT organiza exitoso CyberDrill de la ITU, capacitando a especialistas de ciberseguridad en intensos cuatro días de ejercicios



Marwan Ben Rached, coordinador de ciberseguridad de la ITU; Pablo Palacios; Pelayo Covarrubias; presidente de País Digital; el senador Kenneth Pugh y Daniel Álvarez.

Del lunes al jueves de esta semana tuvo lugar el 12mo CyberDrill de la Unión Internacional de Telecomunicaciones (ITU), realizado por primera vez en Chile y organizado por el CSIRT del Ministerio del Interior, con el apoyo de País Digital y la Universidad de Santiago (USACH), que puso a disposición del evento su Centro de Estudios de Postgrado y Educación Continua en Las Condes.

La apertura contó con la presencia de autoridades como el senador Kenneth Pugh, el subsecretario de Telecomunicaciones, Claudio Araya, oficial de Programas para Sudamérica de la ITU, Pablo Palacios y el coordinador nacional de Ciberseguridad, Daniel Álvarez.



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>

Ciberconsejos | ¿Cómo saber si tu red wifi fue hackeada?

Diversos son los riesgos que pueden existir cuando una red wifi es hackeada. Algunos de ellos son: espionaje, robo de información personal, infección con malware o redirección a sitios falsos. ¿Cómo saber si tu red ha sido intervenida? Te lo contamos en los ciberconsejos de esta semana.

Revísalos aquí: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-wifi-hackeado/>



CIBERCONSEJOS
¿CÓMO SABER SI TU RED WIFI FUE HACKEADA?

1 Internet más lento

Una posible señal de que tu red wifi fue hackeada, es cuando tu conexión a Internet es significativamente más lenta sin razón aparente.

2 Comportamiento extraño

Cuidado si te desconectas repentinamente, tu conexión es inestable o llegas a sitios web falsos, ya que son indicios de que una persona externa podría tener control sobre tu wifi.

Recomendaciones

Si crees que tu red puede estar intervenida o hackeada:

Cambia la contraseña cada cierto tiempo.

¿Cómo crear una contraseña segura?

- Incluye mayúsculas y minúsculas
- Usa números y símbolos
- Crea frases sin sentido y evita usar información personal.

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>

Ciberconsejos | Cybermonday seguro

El lunes 2 de octubre comienza una nueva versión del Cybermonday, evento de ecommerce que congrega a muchas marcas para realizar compras en línea con descuentos respecto de sus precios habituales. Debido a su popularidad y masificación, les recordamos en qué deben fijarse para evitar estafas si desean o necesitan realizar una compra online segura: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-cybermonday-seguro/>



Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA UN CYBERMONDAY SEGURO

#Cybercl

- 1. SI RECIBES UN CORREO** inesperado con enlaces o archivos adjuntos sobre una oferta especial, descártalo, podría tratarse de una estafa de phishing.
- 2. SI BUSCAS** una buena oferta, hazlo directamente en los sitios web oficiales de las tiendas comerciales.



Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA UN CYBERMONDAY SEGURO

#Cybercl

- 3. LOS ATACANTES CREAN** aplicaciones falsas que lucen idénticas a las originales. Si realizas tus compras desde tu Tablet o Smartphone, asegúrate de utilizar aplicaciones confiables.
- 4. ANTES DE COMPRAR** actualiza tus aplicaciones y sistema operativo.



Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA UN CYBERMONDAY SEGURO

#Cybercl

- 5. NO GUARDES** los datos de la forma de pago en tus dispositivos. Si llegas a perderlos, te expones al robo de tus credenciales y a posibles estafas.
- 6. ANTES DE COMPRAR**, analiza los pagos permitidos en el sitio web. Utiliza canales de pago formales.



Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

CIBERCONSEJOS PARA UN CYBERMONDAY SEGURO

#Cybercl

- 7. NUNCA** compartas la información de tus tarjetas de crédito, claves dinámicas o cuentas bancarias.
- 8. ATENCIÓN** al revisar el sitio en el que navegas. Revisa los detalles, como el nombre del dominio y https ya que podría tratarse de un sitio falso.

CONTACTO Y REDES SOCIALES CSIRT

4. 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





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.

- Gabriel Alberto Grobier Romo
- Sebastián M
- Mauricio Hernández Moraga
- Leonardo Jopia
- Jeison Javier Rubiano Ramírez
- Lucas Díaz

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>