



# CSIRT

Equipo de Respuesta ante Incidentes  
de Seguridad Informática

# BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 233

semana del 15 al 21 de diciembre de 2023

# LA SEMANA EN CIFRAS

## IP INFORMADAS

8

IP advertidas en múltiples campañas de phishing y de fraude.



## URL ADVERTIDAS

10

URL asociadas a sitios fraudulentos y campañas de phishing y malware



## PARCHES COMPARTIDOS

198

Las mitigaciones son útiles en productos de Google, Adobe y OpenSSL



# CONTENIDO

|   |    |
|---|----|
| 1. Phishing .....                           | 3  |
| 2. Sitios fraudulentos.....                 | 4  |
| 3. Vulnerabilidades.....                    | 7  |
| 5. Noticias y concientización.....          | 10 |
| 6. Recomendaciones y buenas prácticas ..... | 11 |
| 7. Muro de la Fama .....                    | 12 |

11111<



## 1. Phishing



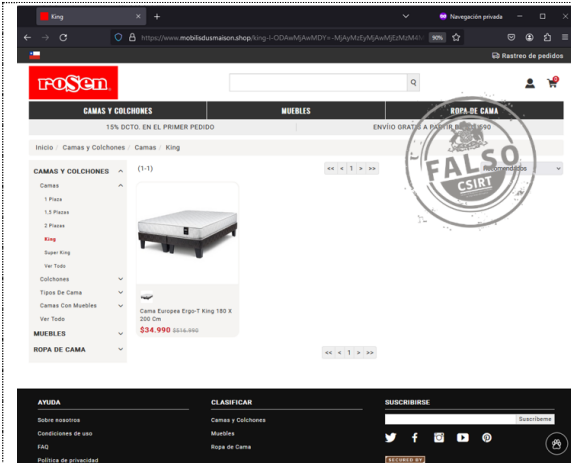
### CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FPH23-00915-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Phishing           |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 19 diciembre, 2023 |
| Última revisión   | 19 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://patito.cdxblocker.ru[.]com/1702998746/imagenes/_personas/home/default.asp">https://patito.cdxblocker.ru[.]com/1702998746/imagenes/_personas/home/default.asp</a> |                    |
| <b>URL de redirección</b>   |                    |
| <a href="https://procontroltotal[.]com/activacion/cuenta-ajwh/">https://procontroltotal[.]com/activacion/cuenta-ajwh/</a>   |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [154.26.158.144]  |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8fph23-00915-01/">https://csirt.gob.cl/alertas/8fph23-00915-01/</a>   |                    |

### CONTACTO Y REDES SOCIALES CSIRT

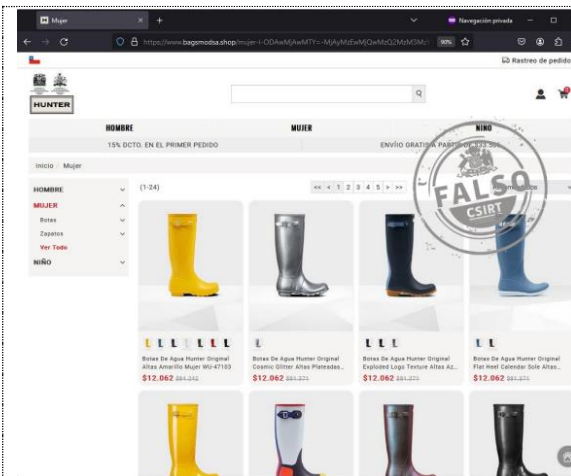
<https://www.csirt.gob.cl>  
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl  
@csirtgob  
<https://www.linkedin.com/company/csirt-gob>

## 2. Sitios fraudulentos



### CSIRT alerta de un nuevo sitio fraudulento que suplanta a Rosen

|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FFR23-01600-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Fraude             |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 19 diciembre, 2023 |
| Última revisión   | 19 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://www.mobilisdusmaison[.]shop/">https://www.mobilisdusmaison[.]shop/</a>                   |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [5.141.156.89]  |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8ffr23-01600-01/">https://csirt.gob.cl/alertas/8ffr23-01600-01/</a> |                    |

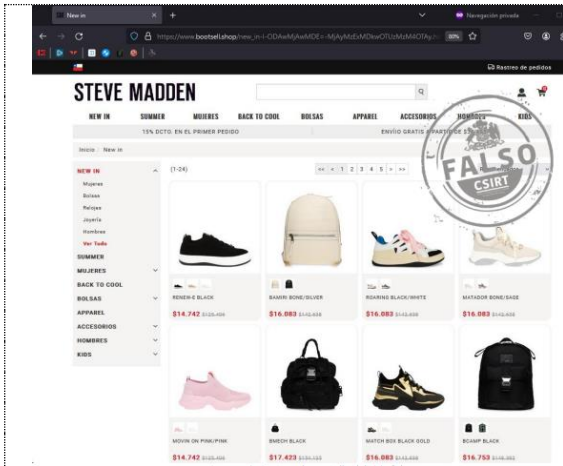


### CSIRT alerta de nuevo sitio fraudulento que suplanta a Hunter

|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FFR23-01601-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Fraude             |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 19 diciembre, 2023 |
| Última revisión   | 19 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://www.bagsmodsa[.]shop/">https://www.bagsmodsa[.]shop/</a>                                 |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [45.141.156.98]   |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8ffr23-01601-01/">https://csirt.gob.cl/alertas/8ffr23-01601-01/</a> |                    |

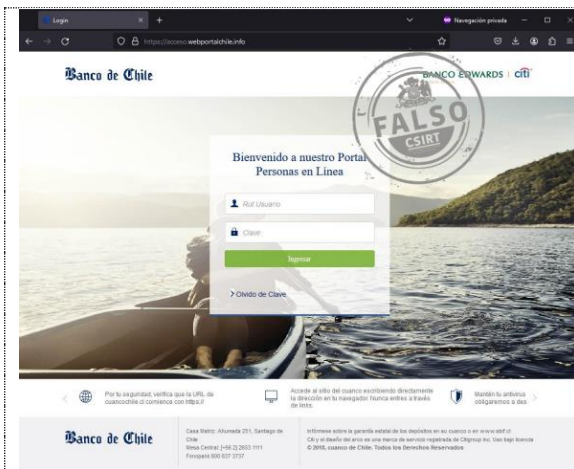
### CONTACTO Y REDES SOCIALES CSIRT

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



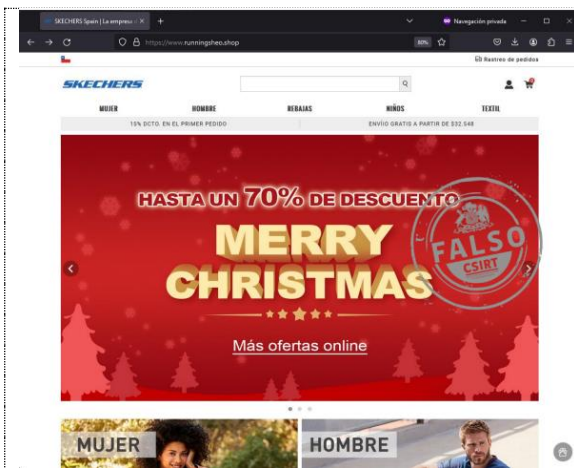
## CSIRT alerta ante nuevo sitio fraudulento que suplanta a Steve Madden

|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FFR23-01602-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Fraude             |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 19 diciembre, 2023 |
| Última revisión   | 19 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://www.bootsell[.]shop">https://www.bootsell[.]shop</a>                                     |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [198.144.149.116]   |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8ffr23-01602-01/">https://csirt.gob.cl/alertas/8ffr23-01602-01/</a> |                    |



## CSIRT alerta de un nuevo sitio fraudulento que suplanta al Banco de Chile

|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FFR23-01603-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Fraude             |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 20 diciembre, 2023 |
| Última revisión   | 20 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://acceso.webportalchile[.]info/">https://acceso.webportalchile[.]info/</a>                 |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [104.21.40.202]   |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8ffr23-01602-01/">https://csirt.gob.cl/alertas/8ffr23-01602-01/</a> |                    |



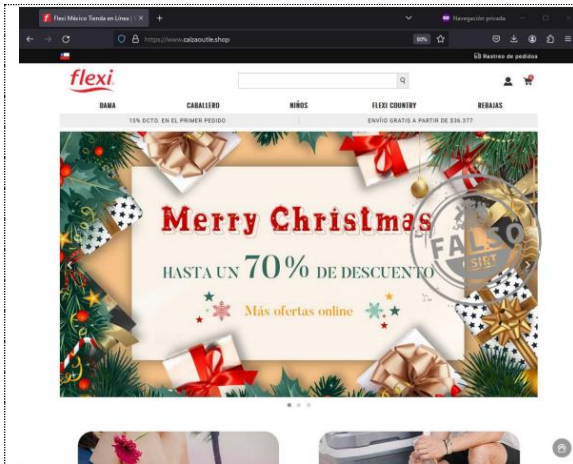
## CSIRT alerta de nuevo sitio fraudulento que suplanta a Skechers

|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FFR23-01604-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Fraude             |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 20 diciembre, 2023 |
| Última revisión   | 20 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://www.runningsheo[.]shop/">https://www.runningsheo[.]shop/</a>                             |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [198.144.149.112]   |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8ffr23-01604-01/">https://csirt.gob.cl/alertas/8ffr23-01604-01/</a> |                    |

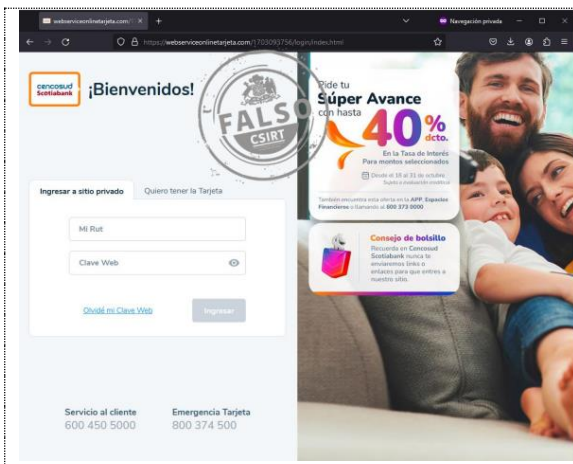
## CSIRT alerta de nuevo sitio fraudulento que suplanta a Flexi

### CONTACTO Y REDES SOCIALES CSIRT

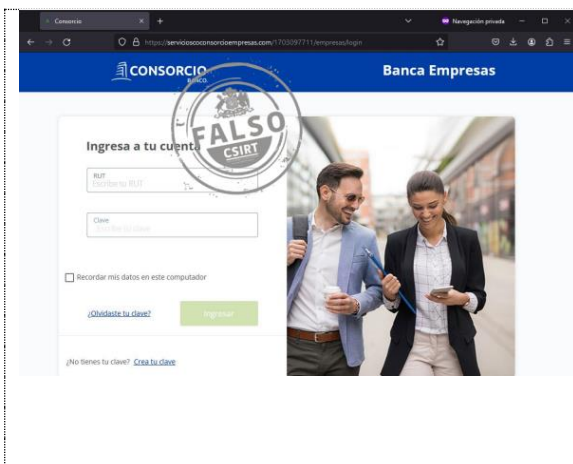
<https://www.csirt.gob.cl>  
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl  
 @csirtgob  
<https://www.linkedin.com/company/csirt-gob>



|                                  |   |
|----------------------------------|---|
| Alerta de seguridad cibernética  | 8FFR23-01605-01   |
| Clase de alerta                  | Fraude  |
| Tipo de incidente                | Fraude  |
| Nivel de riesgo                  | Alto  |
| TLP                              | Blanco  |
| Fecha de lanzamiento original    | 20 diciembre, 2023  |
| Última revisión                  | 20 diciembre, 2023  |
| <b>Indicadores de compromiso</b> |   |
| <b>URL del sitio falso</b>       | <a href="https://www.calzaoutle[.]shop/">https://www.calzaoutle[.]shop/</a>                               |
| <b>Dirección IP sitio falso</b>  | [198.144.149.112]   |
| <b>Enlace para revisar loC:</b>  | <a href="https://csirt.gob.cl/alertas/8ffr23-01605-01/">https://csirt.gob.cl/alertas/8ffr23-01605-01/</a> |



|   |   |
|---|---|
| <b>CSIRT alerta de nuevo sitio fraudulento que suplanta a Cencosud Scotiabank</b> |   |
| Alerta de seguridad cibernética   | 8FFR23-01606-01   |
| Clase de alerta   | Fraude  |
| Tipo de incidente   | Fraude  |
| Nivel de riesgo   | Alto  |
| TLP   | Blanco  |
| Fecha de lanzamiento original   | 20 diciembre, 2023  |
| Última revisión   | 20 diciembre, 2023  |
| <b>Indicadores de compromiso</b>  |   |
| <b>URL del sitio falso</b>  | <a href="https://webserviceonlinetarjeta[.]com/1703093756/login/index.html">https://webserviceonlinetarjeta[.]com/1703093756/login/index.html</a> |
| <b>Dirección IP sitio falso</b>   | [51.79.176.23]  |
| <b>Enlace para revisar loC:</b>   | <a href="https://csirt.gob.cl/alertas/8ffr23-01606-01/">https://csirt.gob.cl/alertas/8ffr23-01606-01/</a>   |



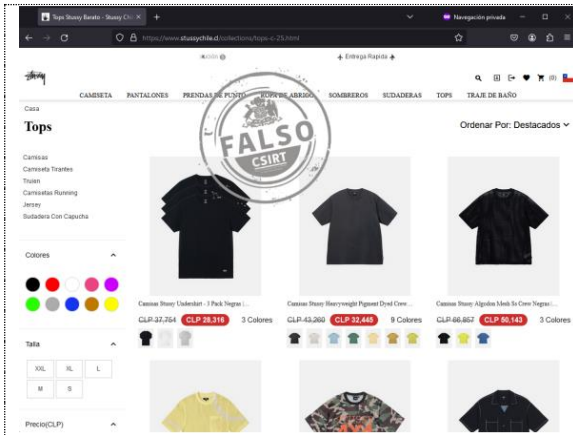
|  |   |
|--|---|
| <b>CSIRT alerta nuevo sitio fraudulento que suplanta a Banco Consorcio</b> |   |
| Alerta de seguridad cibernética  | 8FFR23-01607-01   |
| Clase de alerta  | Fraude  |
| Tipo de incidente  | Fraude  |
| Nivel de riesgo  | Alto  |
| TLP  | Blanco  |
| Fecha de lanzamiento original  | 20 diciembre, 2023  |
| Última revisión  | 20 diciembre, 2023  |
| <b>Indicadores de compromiso</b>   |   |
| <b>URL del sitio falso</b>   | <a href="https://servicioscoconsorcioempresas[.]com/1703097711/empresas/login">https://servicioscoconsorcioempresas[.]com/1703097711/empresas/login</a> |
| <b>Dirección IP sitio falso</b>  | [51.79.176.23]  |
| <b>Enlace para revisar loC:</b>  | <a href="https://csirt.gob.cl/alertas/8ffr23-01607-01/">https://csirt.gob.cl/alertas/8ffr23-01607-01/</a>   |

CSIRT alerta de nuevo sitio fraudulento que suplanta a Stussy

## 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>





|   |                    |
|---|--------------------|
| Alerta de seguridad cibernética   | 8FFR23-01608-01    |
| Clase de alerta   | Fraude             |
| Tipo de incidente   | Fraude             |
| Nivel de riesgo   | Alto               |
| TLP   | Blanco             |
| Fecha de lanzamiento original   | 21 diciembre, 2023 |
| Última revisión   | 21 diciembre, 2023 |
| <b>Indicadores de compromiso</b>  |                    |
| <b>URL del sitio falso</b>  |                    |
| <a href="https://www.stussychile.[.]cl">https://www.stussychile.[.]cl</a>                                 |                    |
| <b>Dirección IP sitio falso</b>   |                    |
| [104.160.25.60]   |                    |
| <b>Enlace para revisar loC:</b>   |                    |
| <a href="https://csirt.gob.cl/alertas/8ffr23-01608-01/">https://csirt.gob.cl/alertas/8ffr23-01608-01/</a> |                    |

## 3. Vulnerabilidades



|   |                              |                |
|---|------------------------------|----------------|
| <b>CSIRT comparte información de vulnerabilidades parchadas por Adobe</b> |                              |                |
| Alerta de seguridad cibernética   | 9VSA23-00944-01              |                |
| Clase de alerta   | Vulnerabilidad               |                |
| Tipo de incidente   | Sistema y/o Software Abierto |                |
| Nivel de riesgo   | Alto                         |                |
| TLP   | Blanco                       |                |
| Fecha de lanzamiento original   | 15 diciembre, 2023           |                |
| Última revisión   | 15 diciembre, 2023           |                |
| <b>CVE</b>  |                              |                |
| CVE-2023-47080  | CVE-2023-48497               | CVE-2023-48562 |
| CVE-2023-47081  | CVE-2023-48498               | CVE-2023-48563 |
| CVE-2023-47074  | CVE-2023-48499               | CVE-2023-48564 |
| CVE-2023-47075  | CVE-2023-48500               | CVE-2023-48565 |
| CVE-2023-47063  | CVE-2023-48501               | CVE-2023-48566 |
| CVE-2023-48632  | CVE-2023-48502               | CVE-2023-48567 |
| CVE-2023-48633  | CVE-2023-48503               | CVE-2023-48568 |
| CVE-2023-48634  | CVE-2023-48504               | CVE-2023-48569 |
| CVE-2023-48635  | CVE-2023-48505               | CVE-2023-48570 |
| CVE-2023-48440  | CVE-2023-48506               | CVE-2023-48571 |
| CVE-2023-48441  | CVE-2023-48507               | CVE-2023-48572 |
| CVE-2023-48442  | CVE-2023-48508               | CVE-2023-48573 |
| CVE-2023-48443  | CVE-2023-48509               | CVE-2023-48574 |
| CVE-2023-48444  | CVE-2023-48510               | CVE-2023-48575 |
| CVE-2023-48445  | CVE-2023-48511               | CVE-2023-48576 |
| CVE-2023-48446  | CVE-2023-48512               | CVE-2023-48577 |
| CVE-2023-48447  | CVE-2023-48513               | CVE-2023-48578 |
| CVE-2023-48448  | CVE-2023-48514               | CVE-2023-48579 |
| CVE-2023-48449  | CVE-2023-48515               | CVE-2023-48580 |
| CVE-2023-48450  | CVE-2023-48516               | CVE-2023-48581 |
| CVE-2023-48451  | CVE-2023-48517               | CVE-2023-48582 |
| CVE-2023-48452  | CVE-2023-48518               | CVE-2023-48583 |
| CVE-2023-48453  | CVE-2023-48519               | CVE-2023-48584 |
| CVE-2023-48454  | CVE-2023-48520               | CVE-2023-48585 |
| CVE-2023-48455  | CVE-2023-48521               | CVE-2023-48586 |
| CVE-2023-48456  | CVE-2023-48522               | CVE-2023-48587 |

## 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>



# Boletín de Seguridad Cibernética N° 233





Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT  
Coordinación Nacional de Ciberseguridad  
Ministerio del Interior y Seguridad Pública  
Gobierno de Chile



BOLETÍN 13BCS23-00242-01 | Semana del 15 de 21 de diciembre de 2023

|  |                |                |
|--|----------------|----------------|
| CVE-2023-48457   | CVE-2023-48523 | CVE-2023-48588 |
| CVE-2023-48458   | CVE-2023-48524 | CVE-2023-48589 |
| CVE-2023-48459   | CVE-2023-48525 | CVE-2023-48590 |
| CVE-2023-48460   | CVE-2023-48526 | CVE-2023-48591 |
| CVE-2023-48461   | CVE-2023-48527 | CVE-2023-48592 |
| CVE-2023-48462   | CVE-2023-48528 | CVE-2023-48593 |
| CVE-2023-48463   | CVE-2023-48529 | CVE-2023-48594 |
| CVE-2023-48464   | CVE-2023-48530 | CVE-2023-48595 |
| CVE-2023-48465   | CVE-2023-48531 | CVE-2023-48596 |
| CVE-2023-48466   | CVE-2023-48532 | CVE-2023-48597 |
| CVE-2023-48467   | CVE-2023-48533 | CVE-2023-48598 |
| CVE-2023-48468   | CVE-2023-48534 | CVE-2023-48599 |
| CVE-2023-48469   | CVE-2023-48535 | CVE-2023-48600 |
| CVE-2023-48470   | CVE-2023-48536 | CVE-2023-48601 |
| CVE-2023-48471   | CVE-2023-48537 | CVE-2023-48602 |
| CVE-2023-48472   | CVE-2023-48538 | CVE-2023-48603 |
| CVE-2023-48473   | CVE-2023-48539 | CVE-2023-48604 |
| CVE-2023-48474   | CVE-2023-48540 | CVE-2023-48605 |
| CVE-2023-48475   | CVE-2023-48541 | CVE-2023-48606 |
| CVE-2023-48476   | CVE-2023-48542 | CVE-2023-48607 |
| CVE-2023-48477   | CVE-2023-48543 | CVE-2023-48608 |
| CVE-2023-48478   | CVE-2023-48544 | CVE-2023-48609 |
| CVE-2023-48479   | CVE-2023-48545 | CVE-2023-48610 |
| CVE-2023-48480   | CVE-2023-48546 | CVE-2023-48611 |
| CVE-2023-48481   | CVE-2023-48547 | CVE-2023-48612 |
| CVE-2023-48482   | CVE-2023-48548 | CVE-2023-48613 |
| CVE-2023-48483   | CVE-2023-48549 | CVE-2023-48614 |
| CVE-2023-48484   | CVE-2023-48550 | CVE-2023-48615 |
| CVE-2023-48485   | CVE-2023-48551 | CVE-2023-48616 |
| CVE-2023-48486   | CVE-2023-48552 | CVE-2023-48617 |
| CVE-2023-48487   | CVE-2023-48553 | CVE-2023-48618 |
| CVE-2023-48488   | CVE-2023-48554 | CVE-2023-48619 |
| CVE-2023-48489   | CVE-2023-48555 | CVE-2023-48620 |
| CVE-2023-48490   | CVE-2023-48556 | CVE-2023-48621 |
| CVE-2023-48491   | CVE-2023-48557 | CVE-2023-48622 |
| CVE-2023-48492   | CVE-2023-48558 | CVE-2023-48623 |
| CVE-2023-48493   | CVE-2023-48559 | CVE-2023-48624 |
| CVE-2023-48494   | CVE-2023-48560 | CVE-2023-47064 |
| CVE-2023-48495   | CVE-2023-48561 | CVE-2023-47065 |
| CVE-2023-48496   |                |                |
| <b>Fabricante</b>  |                |                |
| Adobe  |                |                |
| <b>Productos afectados</b>   |                |                |
| Illustrator 2024 28.0 y anteriores.<br>Illustrator 2023 27.9 y anteriores.<br>Adobe After Effects 24.0.3 y anteriores<br>Adobe After Effects 23.6.0 y anteriores.<br>Adobe Substance 3D Stager 2.1.1 y anteriores.<br>Adobe Experience Manager (AEM).<br>AEM Cloud Service (CS) 6.5.18.0 y anteriores. |                |                |
| <b>Enlaces para revisar el informe:</b>  |                |                |
| <a href="https://csirt.gob.cl/vulnerabilidades/9vsa23-00944-01/">https://csirt.gob.cl/vulnerabilidades/9vsa23-00944-01/</a>  |                |                |

## CONTACTO Y REDES SOCIALES CSIRT

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



Ministerio del Interior y Seguridad Pública

## INFORME DE Vulnerabilidad

**9VSA23-00945-01**  
CSIRT comparte datos de actualización día cero en Google Chrome

PARA REGISTRAR | 1510  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)



Equipo de Respuesta ante Incidentes de Seguridad Informática

### CSIRT comparte información de una nueva vulnerabilidad de día cero parchada para Google Chrome

|                                 |                              |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00945-01              |
| Clase de alerta                 | Vulnerabilidad               |
| Tipo de incidente               | Sistema y/o Software Abierto |
| Nivel de riesgo                 | Alto                         |
| TLP                             | Blanco                       |
| Fecha de lanzamiento original   | 21 diciembre, 2023           |
| Última revisión                 | 21 diciembre, 2023           |

#### CVE

CVE-2023-7024

#### Fabricante

Google Chrome

#### Productos afectados

Google Chrome, todas las versiones anteriores a la 120.0.6099.129 para Mac y Linux y 120.0.6099.129/130 para Windows.

#### Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa23-00945-01/>



Ministerio del Interior y Seguridad Pública

## INFORME DE Vulnerabilidad

**9VSA23-00946-01**  
CSIRT comparte información de dos vulnerabilidades parchadas en OpenSSL 9.6

PARA REGISTRAR | 1510  
UN INCIDENTE | [www.csirt.gob.cl](http://www.csirt.gob.cl)



Equipo de Respuesta ante Incidentes de Seguridad Informática

### CSIRT comparte información de dos vulnerabilidades parchadas en OpenSSL 9.6

|                                 |                              |
|---------------------------------|------------------------------|
| Alerta de seguridad cibernética | 9VSA23-00946-01              |
| Clase de alerta                 | Vulnerabilidad               |
| Tipo de incidente               | Sistema y/o Software Abierto |
| Nivel de riesgo                 | Alto                         |
| TLP                             | Blanco                       |
| Fecha de lanzamiento original   | 21 diciembre, 2023           |
| Última revisión                 | 21 diciembre, 2023           |

#### CVE

CVE-2023-48795

CVE-2023-51385

#### Fabricante

OpenSSL

#### Productos afectados

OpenSSH anteriores a 9.6.

#### Enlaces para revisar el informe:

<https://csirt.gob.cl/vulnerabilidades/9vsa23-00946-01/>

## CONTACTO Y REDES SOCIALES CSIRT

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

## 5. Noticias y concientización

### Ciberconsejos | Manual para unas vacaciones seguras

Prepárate para estas vacaciones, protege a tu organización y capacita a tus equipos para evitar caer en ataques cibernéticos durante el verano con el siguiente manual que preparamos para los ciberconsejos de esta semana, con recomendaciones sobre los principales aspectos a considerar para cuidar el correo electrónico, configurar las VPN, mejorar la creación y uso de contraseñas y elaborar un plan de concientización efectivo, todas acciones necesarias para mejorar la ciberseguridad de nuestras instituciones e incluso nuestros hogares.

Ver más: <https://csirt.gob.cl/recomendaciones/ciberconsejos-vacaciones-2024/>







## BUENAS PRÁCTICAS

### Medidas de ciberseguridad en vacaciones



#### 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>



## 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

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





## 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.

- Miguel Morales
- Felipe Pavez
- Francisco Carvajal
- Gustavo Soto

### CONTACTO Y REDES SOCIALES CSIRT

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