



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 211

semana del 14 al 20 de julio de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

10

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

16

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

59

Las mitigaciones son útiles en productos de Adobe, Citrix, Woo, Juniper y SonicWall.



HASH REPORTADOS

4

Hashes asociados a múltiples campañas de phishing con archivos que contienen malware



CONTENIDO

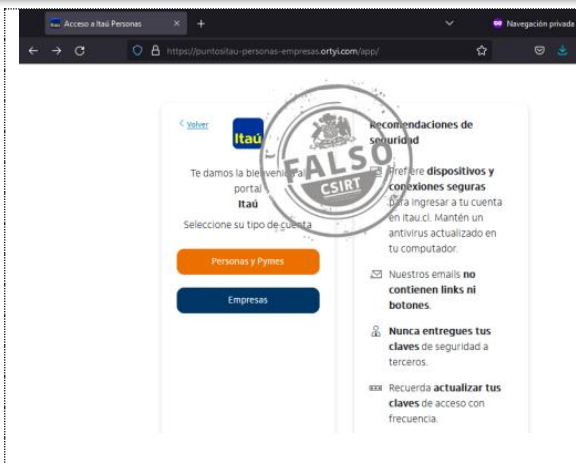
1.	Sitios fraudulentos	3
2.	Phishing	6
3.	Malware.....	7
4.	Vulnerabilidades	8
5.	Concientización.....	11
6.	Recomendaciones y buenas prácticas	13
7.	Muro de la Fama	14



CSIRT

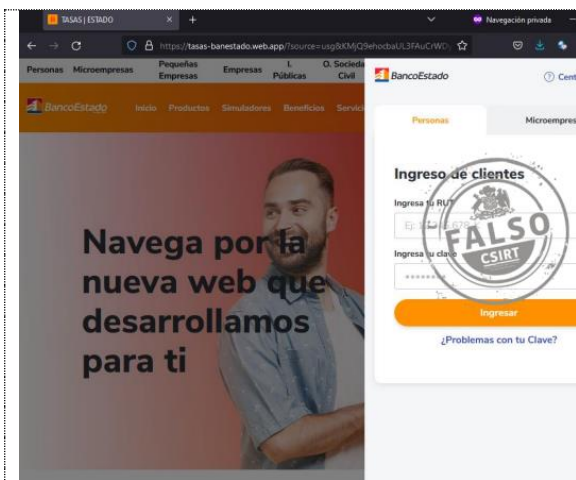
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos



CSIRT alerta ante nuevo sitio fraudulento que suplanta a Banco Itaú

Alerta de seguridad cibernética	8FFR23-01461-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 julio, 2023
Última revisión	14 julio, 2023
Indicadores de compromiso	
URL sitio falso	https://puntositaú-personas-empresas.ortyi[.]com/app/
Dirección IP	[172.67.187.186]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01461-01/



CSIRT alerta ante nuevo sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FFR23-01462-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 julio, 2023
Última revisión	17 julio, 2023
Indicadores de compromiso	
URL sitio falso	https://bit[.]ly/3omdStp https://tasas-banestado.web[.]app/?source
Dirección IP	[199.36.158.100]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01462-01/

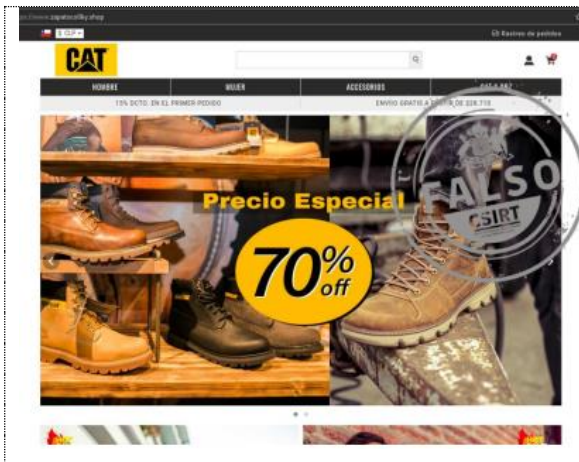


CSIRT alerta de nueva página fraudulenta que suplanta a ABCDin

Alerta de seguridad cibernética	8FFR23-01463-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 julio, 2023
Última revisión	17 julio, 2023
Indicadores de compromiso	
URL sitio falso	https://abcdinchile.myshopify[.]com
Dirección IP	[23.227.38.74]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01463-01/

CONTACTO Y REDES SOCIALES CSIRT

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



CSIRT alerta ante nuevo sitio fraudulento que suplanta a Caterpillar

Alerta de seguridad cibernética	8FFR23-01464-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 julio, 2023
Última revisión	17 julio, 2023

Indicadores de compromiso

URL sitio falso

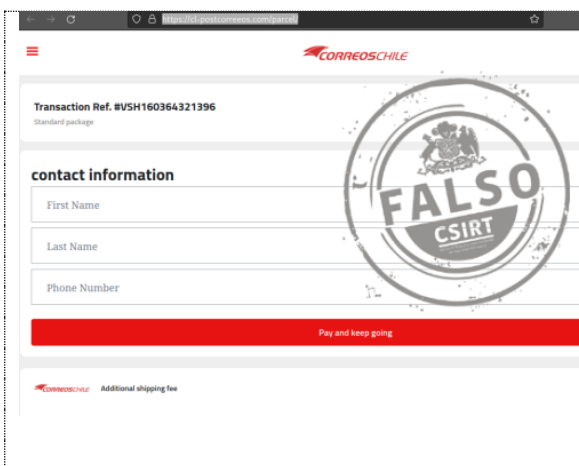
[https://www.zapatocollky\[.\]shop/](https://www.zapatocollky[.]shop/)

Dirección IP

[199.21.150.26]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01464-01/>



CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile

Alerta de seguridad cibernética	8FFR23-01465-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 julio, 2023
Última revisión	17 julio, 2023

Indicadores de compromiso

URL sitio falso

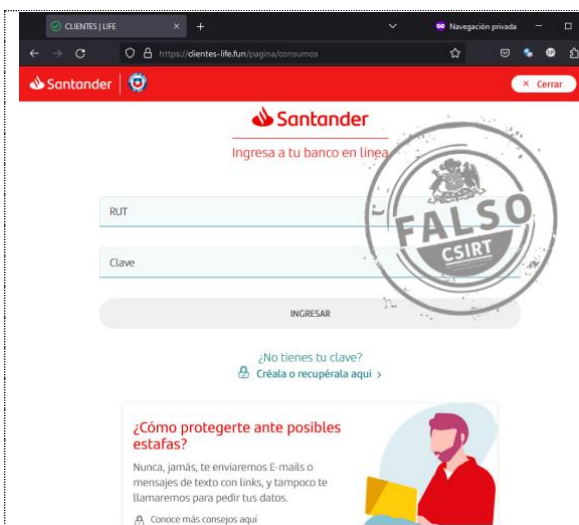
[https://cl-postcorreos\[.\]com/parcel/](https://cl-postcorreos[.]com/parcel/)

Dirección IP

[89.117.169.118]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01465-01/>



CSIRT alerta ante nueva página fraudulenta que suplanta a Banco Santander

Alerta de seguridad cibernética	8FFR23-01466-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 julio, 2023
Última revisión	18 julio, 2023

Indicadores de compromiso

URL sitio falso

[https://clientes-life\[.\]fun/pagina/consumos](https://clientes-life[.]fun/pagina/consumos)

Dirección IP

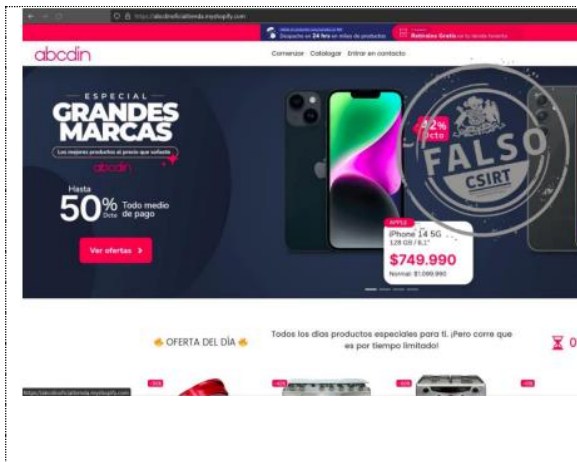
[104.21.53.200]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01466-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



CSIRT informa de nuevo sitio fraudulento que suplanta a ABCDin

Alerta de seguridad cibernética	8FFR23-01467-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 julio, 2023
Última revisión	18 julio, 2023

Indicadores de compromiso

URL sitio falso

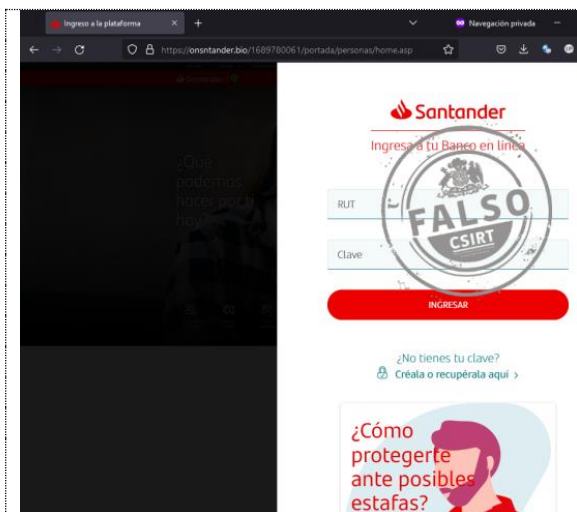
[https://abcdinoficialtienda.myshopify\[.\]com/](https://abcdinoficialtienda.myshopify[.]com/)

Dirección IP

N/D

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01467-01/>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Banco Santander

Alerta de seguridad cibernética	8FFR23-01468-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 julio, 2023
Última revisión	18 julio, 2023

Indicadores de compromiso

URL sitio falso

[https://onsntander\[.\]bio/1689780061/portada/personas/home.asp](https://onsntander[.]bio/1689780061/portada/personas/home.asp)

Dirección IP

[104.21.44.158]

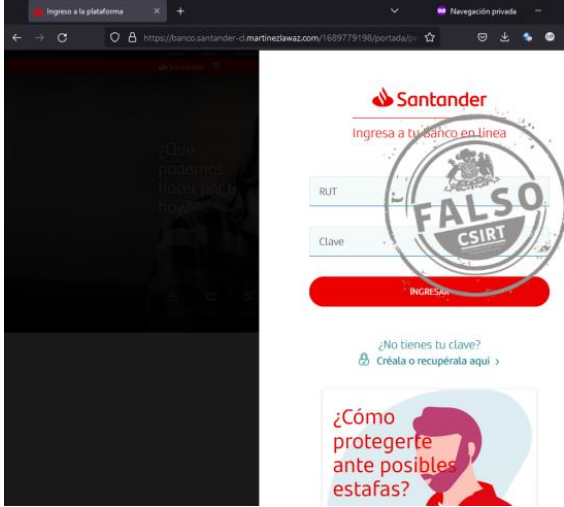
Enlace para revisar el informe:


<https://www.csirt.gob.cl/alertas/8ffr23-01468-01/>

CONTACTO Y REDES SOCIALES CSIRT


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

2. Phishing

	<p>CSIRT alerta de nueva campaña de phishing que suplanta a Banco Santander</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00856-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>19 julio, 2023</td> </tr> <tr> <td>Última revisión</td> <td>19 julio, 2023</td> </tr> </table> <p>URL redirección https://bit[.]ly/43wntwz?l=www.santander.cl https://nationaltreasures[.]co.nz/bancosantander/cuenta-hzkh/</p> <p>URL sitio falso https://banco.santander-cl.martinezlawaz[.]com/1689779198/portada/personas/home.asp</p> <p>Dirección IP [107.190.131.66]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00856-01/</p>	Alerta de seguridad cibernética	8FPH23-00856-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	19 julio, 2023	Última revisión	19 julio, 2023
Alerta de seguridad cibernética	8FPH23-00856-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	19 julio, 2023														
Última revisión	19 julio, 2023														

	<p>CSIRT alerta de nueva campaña de phishing, que suplanta a BancoEstado</p> <table border="1"> <tr> <td>Alerta de seguridad cibernética</td> <td>8FPH23-00857-01</td> </tr> <tr> <td>Clase de alerta</td> <td>Fraude</td> </tr> <tr> <td>Tipo de incidente</td> <td>Phishing</td> </tr> <tr> <td>Nivel de riesgo</td> <td>Alto</td> </tr> <tr> <td>TLP</td> <td>Blanco</td> </tr> <tr> <td>Fecha de lanzamiento original</td> <td>19 julio, 2023</td> </tr> <tr> <td>Última revisión</td> <td>19 julio, 2023</td> </tr> </table> <p>Indicadores de compromiso</p> <p>URL redirección https://lolocontac[.]com/activacion/cuenta-qgah/</p> <p>URL sitio falso https://bandafongape[.]com/1689790630/imagenes/_personas/home/default.asp</p> <p>Dirección IP sitio falso [64.37.50.234]</p> <p>Enlace para revisar loC: https://www.csirt.gob.cl/alertas/8fph23-00857-01/</p>	Alerta de seguridad cibernética	8FPH23-00857-01	Clase de alerta	Fraude	Tipo de incidente	Phishing	Nivel de riesgo	Alto	TLP	Blanco	Fecha de lanzamiento original	19 julio, 2023	Última revisión	19 julio, 2023
Alerta de seguridad cibernética	8FPH23-00857-01														
Clase de alerta	Fraude														
Tipo de incidente	Phishing														
Nivel de riesgo	Alto														
TLP	Blanco														
Fecha de lanzamiento original	19 julio, 2023														
Última revisión	19 julio, 2023														

CONTACTO Y REDES SOCIALES CSIRT

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

3. Malware

	CSIRT alerta de nueva campaña de phishing con malware en falsa cotización	
	Alerta de seguridad cibernética	2CMV23-00426-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	18 julio, 2023
	Última revisión	18 julio, 2023
	Indicadores de compromiso	
	URL-Dominio	
http://195.178.120[.]24/PPZrQQAxIGIYpWRhmWDcUPp.vbs http://servidorarquivos.duckdns[.]org/e/e		
SHA256		
6cf5eb81d932e600c8ca6662cdd81fad871d2a31733a39154862062782d1a58b650ae74cf998803602f93dbcc56b25ccb13b4d45914be507511cbf5fe619007f7c451d9ecb10e2a1aa4512e56ab3859675ab3f28aa40d3c63e45e4e8c35b10cb0ace5259a5f3de5bfd71221aac959b8054bc31018aac425aa440aa4fe451ebb8		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/alertas/2cmv23-00426-01/		

CONTACTO Y REDES SOCIALES CSIRT

4. Vulnerabilidades



CSIRT comparte vulnerabilidades parchadas por Juniper Networks en Junos OS

Alerta de seguridad cibernética	9VSA23-00863-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 julio, 2023
Última revisión	13 julio, 2023

CVE		
CVE-2022-31629	CVE-2017-7654	CVE-2022-41974
CVE-2022-31628	CVE-2017-7655	CVE-2022-42898
CVE-2022-31627	CVE-2020-13817	CVE-2021-26401
CVE-2022-31626	CVE-2020-11868	CVE-2022-2964
CVE-2022-31625	CVE-2019-11358	CVE-2020-13946
CVE-2021-21708	CVE-2021-40085	CVE-2022-38023
CVE-2021-21707	CVE-2022-23825	CVE-2022-42703
CVE-2021-21705	CVE-2022-2588	CVE-2022-4378
CVE-2021-21704	CVE-2022-26373	CVE-2021-25220
CVE-2021-21703	CVE-2022-29900	CVE-2022-2795
CVE-2021-21702	CVE-2022-29901	CVE-2023-36838
CVE-2020-7071	CVE-2022-30123	CVE-2023-36849
CVE-2017-7653	CVE-2022-3276	CVE-2023-36835

Fabricante
Juniper

Productos afectados
Juniper Networks Junos OS, todas las versiones.
Juniper Networks Junos OS Evolved, todas las versiones.
Juniper Networks Junos Space.

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00863-01/>



CSIRT comparte información de vulnerabilidad crítica en Adobe ColdFusion, que está siendo explotada

Alerta de seguridad cibernética	9VSA23-00864-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 julio, 2023
Última revisión	17 julio, 2023

CVE
CVE-2023-29300

Fabricante
Adobe

Productos afectados
Servidores Coldfusion 2018, 2021 y 2023.

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00864-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00865-01
CSIRT informa de vulnerabilidades críticas en SonicWall GMS y Analytics

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



CSIRT comparte información de vulnerabilidades críticas en SonicWall GMS y Analytics

Alerta de seguridad cibernética	9VSA23-00865-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 julio, 2023
Última revisión	17 julio, 2023

CVE

CVE-2023-34123	CVE-2023-34128	CVE-2023-34133
CVE-2023-34124	CVE-2023-34129	CVE-2023-34134
CVE-2023-34125	CVE-2023-34130	CVE-2023-34135
CVE-2023-34126	CVE-2023-34131	CVE-2023-34136
CVE-2023-34127	CVE-2023-34132	CVE-2023-34137

Fabricante

SonicWall

Productos afectados

SonicWall GMS 9.3.2-SP1 y anteriores.
SonicWall Analytics 2.5.0.4-R7 y anteriores.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00865-01/>



Ministerio del Interior y Seguridad Pública

INFORME DE Vulnerabilidad

9VSA23-00866-01
CSIRT informa de vulnerabilidad crítica explotada en WooCommerce para Wordpress

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



CSIRT informa vulnerabilidad crítica explotada en WooCommerce para Wordpress

Alerta de seguridad cibernética	9VSA23-00866-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 julio, 2023
Última revisión	18 julio, 2023

CVE

CVE-2023-28121

Fabricante

Woo

Productos afectados

WooCommerce, versiones anteriores a la 5.6.2, que parcha esta vulnerabilidad.

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00866-01/>

CONTACTO Y REDES SOCIALES CSIRT

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



CSIRT informa de tres vulnerabilidades en NetScaler de Citrix, una crítica

Alerta de seguridad cibernética	9VSA23-00867-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 julio, 2023
Última revisión	18 julio, 2023

CVE

CVE-2023-3519
CVE-2023-3466
CVE-2023-3467

Fabricante

Citrix

Productos afectados

NetScaler ADC y NetScaler Gateway anteriores a la versión 13.1-49.13
NetScaler ADC y NetScaler Gateway anteriores a la versión 13.0-91.13
NetScaler ADC anteriores a la versión 13.1-FIPS 13.1-37.159
NetScaler ADC anteriores a la versión 12.1-FIPS 12.1-65.36
NetScaler ADC anteriores a la versión 12.1-NDcPP 12.1-65.36

Enlaces para revisar el informe:

<https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00867-01/>

CONTACTO Y REDES SOCIALES CSIRT

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

5. Concientización

Ciberconsejos para el uso seguro de las cookies

Las cookies son pequeños archivos de texto que el navegador almacena en el disco duro de cada computador al visitar un sitio web. Para qué sirven, sus riesgos y cómo usarlas de forma adecuada, fueron las preguntas que respondimos en los Ciberconsejos de esta semana, los que pueden también ser vistos aquí: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-cookies/>.



The infographic is divided into four quadrants, each with the CSIRT logo. The top-left quadrant, titled '¿Qué son las cookies?', explains that cookies are small text files stored on a computer and that they allow websites to remember user information. The top-right quadrant, 'Riesgos de las cookies', lists three risks: 1. Privacy: websites can track online activity; 2. Information storage: websites can store personal data like email addresses, which could be stolen; 3. Invasive advertising: cookies can be used to target ads based on user behavior. The bottom-left quadrant, 'Algunos usos de las cookies', lists four uses: 1. Saving login credentials; 2. Keeping items in a shopping cart; 3. Remembering the last visit date; 4. Enabling personalized advertising. The bottom-right quadrant, 'Recomendaciones', lists three recommendations: 1. Configure the browser to reject third-party cookies; 2. Delete cookies regularly; 3. Use private or incognito browsing. The bottom-right quadrant has a purple background, while the others are light grey.




CONTACTO Y REDES SOCIALES CSIRT

Ciberdiccionario Volumen 40

Compartimos esta semana con nuestra comunidad una nueva publicación del Ciberdiccionario, esta vez en su volumen 40 con los conceptos de filtrado de paquetes, sniffer, BYOD (“bring your own device”) y autenticación. Encuentrenlo también aquí: <https://www.csirt.gov.cl/recomendaciones/ciberdiccionario-volumen-40/>.

 <h3>Ciber diccionario</h3> <h4>Filtrado de paquetes</h4> <p>Corresponde al proceso de examinar y controlar el tráfico de red que ingresa o sale de la misma, con el objetivo de protegerla contra amenazas o ataques, además de controlar el correcto consumo de ancho de banda. Esto es realizado por equipos de red (firewall o enrutadores) que se basan en diversos criterios configurados para filtrar, por ejemplo: Dirección IP de origen, IP de destino, protocolos, etc.</p> 	 <h3>Ciber diccionario</h3> <h4>Sniffer</h4> <p>Programa que captura y analiza en tiempo real el tráfico de la red. Son utilizados para detectar actividades sospechosas, identificar amenazas o vulnerabilidades y aplicar medidas de seguridad. Por otro lado, también son usados con fines maliciosos, principalmente para el espionaje del tráfico de terceras personas. Su nombre viene del inglés "rastreador" o "husmeador".</p> 
 <h3>Ciber diccionario</h3> <h4>Autenticación</h4> <p>Proceso de verificación y confirmación de la identidad de un usuario. Para eso, el individuo debe proveer algo que sabe (como una contraseña o un PIN), algo que tenga (como una tarjeta de coordenadas o un token) o algo que sepa (identificación biométrica o dinámicas de tecleo, por ejemplo). Lo ideal es que la autenticación requiera verificar al menos dos de estas condiciones (autenticación multifactor).</p> 	 <h3>Ciber diccionario</h3> <h4>BYOD</h4> <p>Sigla de “bring your own device” en inglés, o sea, “traiga su propio dispositivo”. Se usa en instituciones que no entregan a sus trabajadores un equipo (computadores o smartphones) para realizar su labor, debiendo emplear aparatos de su propiedad. Implementar BYOD involucra tomar medidas para resguardar la seguridad y privacidad de la información que pasa por estos equipos.</p> 

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gov.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: soc@interior.gov.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: soc@interior.gob.cl
 [@csirtgob](https://twitter.com/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
- Nicolás Fernández
- Julio César Muñoz Strauss
- Didye Paolo Orellana Ponce
- Josefa Belén Contreras Piña
- Francisco Javier Flores Varela
- Gonzalo Andrés Araya Navarrete

CONTACTO Y REDES SOCIALES CSIRT

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