



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 217

semana del 25 al 31 de agosto de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

15

IP advertidas en múltiples campañas de phishing y de fraude.



URL ADVERTIDAS

19

URL asociadas a sitios fraudulentos y campañas de phishing y malware



PARCHES COMPARTIDOS

26

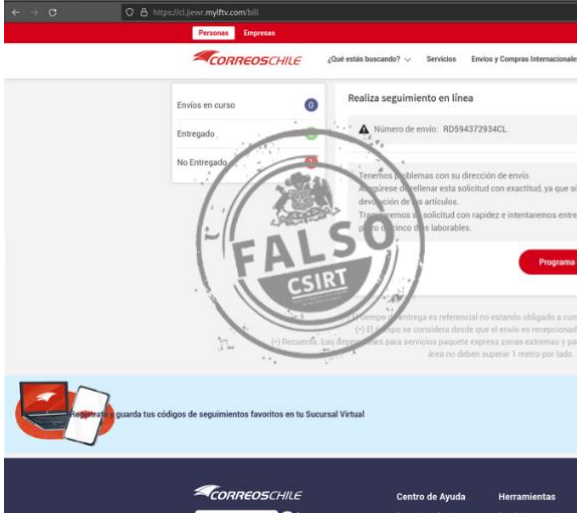
Las mitigaciones son útiles en productos de Mozilla, Cisco, VMware y Google.



CONTENIDO

1.	Sitios fraudulentos	3
2.	Phishing	8
3.	Vulnerabilidades	9
4.	Noticias y concientización	11
5.	Recomendaciones y buenas prácticas	16
6.	Muro de la Fama	17

1. Sitios fraudulentos

	CSIRT alerta de sitio fraudulento que suplanta a BancoEstado	
	Alerta de seguridad cibernética	8FFR23-01501-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	26 agosto, 2023
	Última revisión	26 agosto, 2023
	Indicadores de compromiso	
	URL sitio falso	https://cl.jiewr.myfltv[.]com/bill
URL de redirección	https://qrco[.]de/beGdLI	
IP del sitio falso	[43.153.106.5]	
Enlace para revisar el informe:		
https://www.csirt.gob.cl/alertas/8ffr23-01501-01/		

	CSIRT alerta de nuevo sitio falso que suplanta a ABCDin	
	Alerta de seguridad cibernética	8FFR23-01502-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	26 agosto, 2023
	Última revisión	26 agosto, 2023
	Indicadores de compromiso	
	URL sitio falso	https://abcdinpagos.myshopify[.]com/
Dirección IP	N/A	
Enlace para revisar el informe:		
https://www.csirt.gob.cl/alertas/8ffr23-01502-01/		

	CSIRT alerta de nuevo sitio fraudulento que suplanta a Linio	
	Alerta de seguridad cibernética	8FFR23-01503-01
	Clase de alerta	Fraude
	Tipo de incidente	Falsificación de Registros o Identidad
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	26 agosto, 2023
	Última revisión	26 agosto, 2023
	Indicadores de compromiso	
	URL sitio falso	https://www.qlyrow.com/
Dirección IP	[47.89.219.149]	
Enlace para revisar el informe:		
https://www.csirt.gob.cl/alertas/8ffr23-01503-01/		

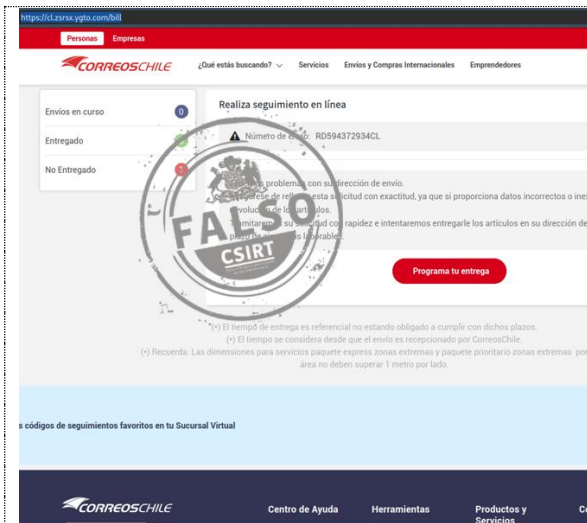
CONTACTO Y REDES SOCIALES CSIRT

Boletín de Seguridad Cibernética N° 217

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



BOLETÍN 13BCS23-00226-01 | Semana del 25 al 31 de agosto de 2023



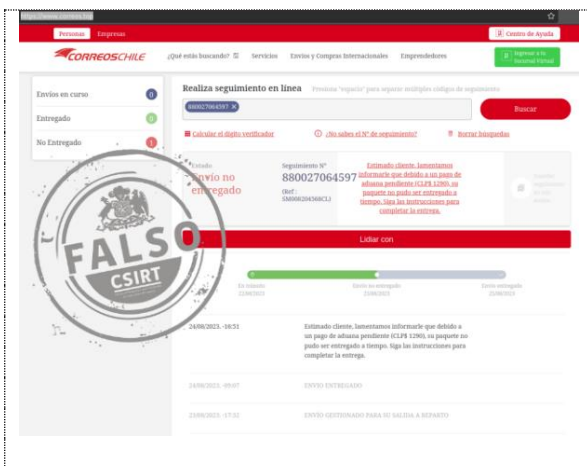
CSIRT alerta ante nueva página fraudulenta que suplanta a CorreosChile

Alerta de seguridad cibernética	8FFR23-01504-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 agosto, 2023
Última revisión	26 agosto, 2023
Indicadores de compromiso	
URL sitio falso	https://cl.zsrsx.ygto.com/bill
URL de redirección	qrco.de/beHCif
Dirección IP	[43.153.106.5]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01504-01/



CSIRT alerta de nuevo sitio fraudulento que suplanta a ABC Visa

Alerta de seguridad cibernética	8FFR23-01505-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 agosto, 2023
Última revisión	26 agosto, 2023
Indicadores de compromiso	
URL sitio falso	https://abcserviciosfinancieros-cl.gmjs[.]org/
URL de redirección	N/A
Dirección IP	[72.46.128.210]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01505-01/



CSIRT alerta de nueva página fraudulenta que suplanta a CorreosChile

Alerta de seguridad cibernética	8FFR23-01506-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 agosto, 2023
Última revisión	26 agosto, 2023
Indicadores de compromiso	
URL sitio falso	https://www.correos.top/
Dirección IP	[170.106.106.43]
Enlace para revisar el informe:	https://www.csirt.gob.cl/alertas/8ffr23-01506-01/

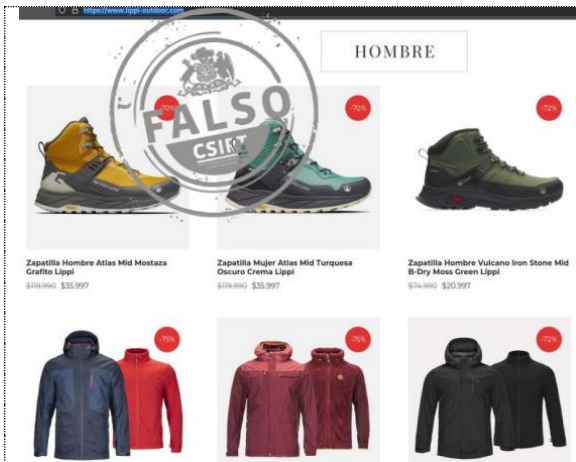
CONTACTO Y REDES SOCIALES CSIRT

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

Boletín de Seguridad Cibernética N° 217

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

BOLETÍN 13BCS23-00226-01 | Semana del 25 al 31 de agosto de 2023

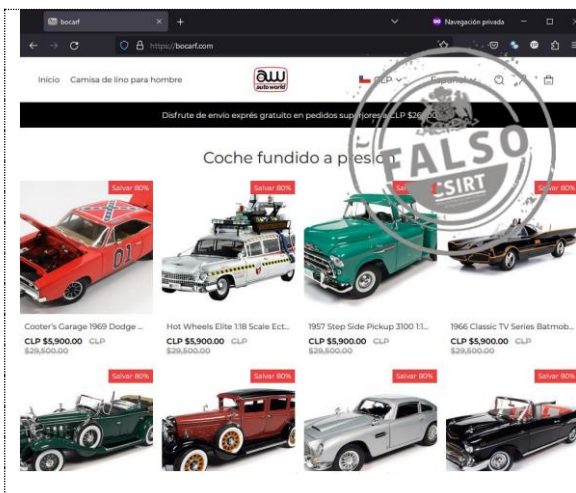


CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi

Alerta de seguridad cibernética	8FFR23-01507-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 agosto, 2023
Última revisión	26 agosto, 2023

Indicadores de compromiso

URL sitio falso
<https://www.lippi-outdoor.com/>
Dirección IP
 [104.21.43.224]
Enlace para revisar el informe:
<https://www.csirt.gob.cl/alertas/8ffr23-01507-01/>

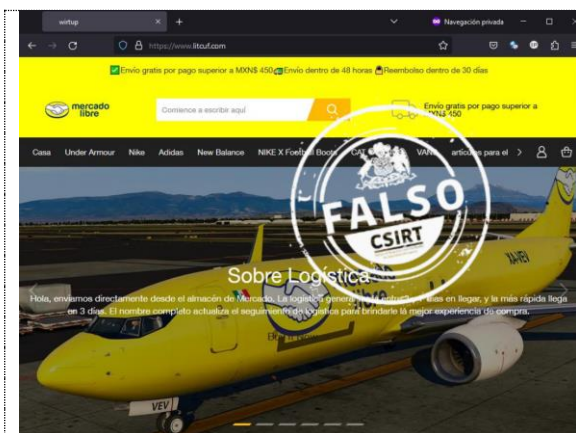


CSIRT alerta de activación de sitio fraudulento que simula ser tienda de autitos de colección

Alerta de seguridad cibernética	8FFR23-01508-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 agosto, 2023
Última revisión	29 agosto, 2023

Indicadores de compromiso

URL sitio falso
<https://bocarf.com/>
Dirección IP
 [47.89.219.149]
Enlace para revisar el informe:
<https://www.csirt.gob.cl/alertas/8ffr23-01508-01/>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Mercado Libre

Alerta de seguridad cibernética	8FFR23-01509-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 agosto, 2023
Última revisión	29 agosto, 2023

Indicadores de compromiso

URL sitio falso
<https://www.litcuf.com/>
Dirección IP
 [47.89.219.149]
Enlace para revisar el informe:
<https://www.csirt.gob.cl/alertas/8ffr23-01509-01/>

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>

Boletín de Seguridad Cibernética N° 217

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

BOLETÍN 13BCS23-00226-01 | Semana del 25 al 31 de agosto de 2023

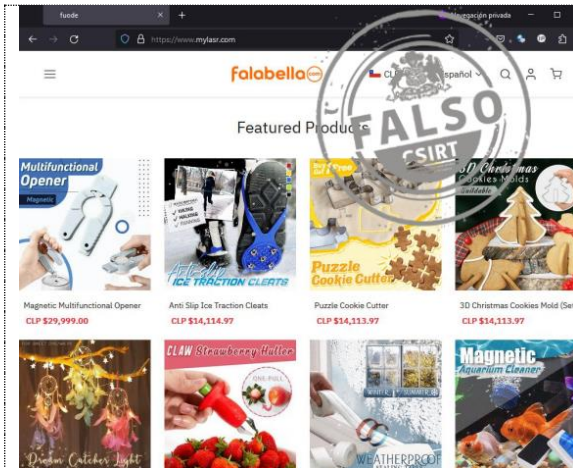


CSIRT alerta de nuevo sitio fraudulento que suplanta a Mercado Libre

Alerta de seguridad cibernética	8FFR23-01510-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 agosto, 2023
Última revisión	29 agosto, 2023

Indicadores de compromiso

URL sitio falso
 crupla.com
Dirección IP
 [47.89.219.149]
Enlace para revisar el informe:
<https://www.csirt.gob.cl/alertas/8ffr23-01510-01/>

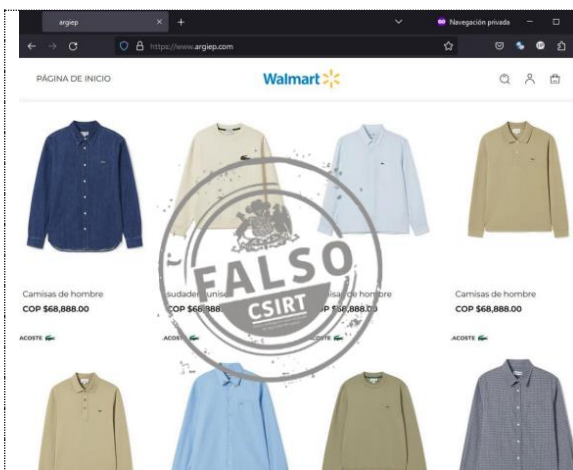


CSIRT alerta de nuevo sitio fraudulento que suplanta a Falabella

Alerta de seguridad cibernética	8FFR23-01511-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 agosto, 2023
Última revisión	29 agosto, 2023

Indicadores de compromiso

URL sitio falso
<https://www.mylasr.com/>
Dirección IP
 [47.89.219.149]
Enlace para revisar el informe:
<https://www.csirt.gob.cl/alertas/8ffr23-01511-01/>



CSIRT alerta de nuevo sitio fraudulento que suplanta a Walmart

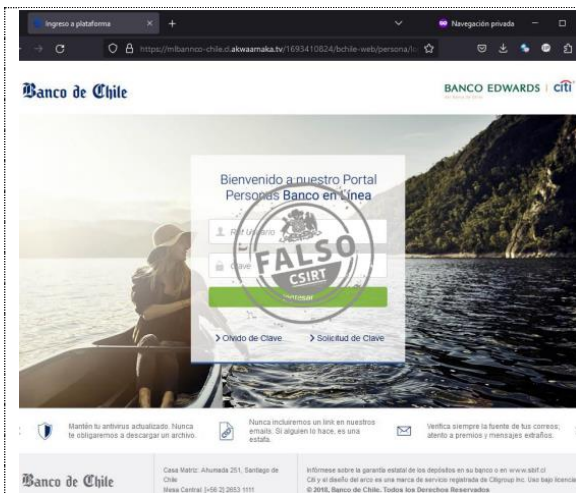
Alerta de seguridad cibernética	8FFR23-01512-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 agosto, 2023
Última revisión	29 agosto, 2023

Indicadores de compromiso

URL sitio falso
<https://www.argiep.com/>
Dirección IP
 [47.89.219.149]
Enlace para revisar el informe:
<https://www.csirt.gob.cl/alertas/8ffr23-01512-01/>

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 alerta de nueva página fraudulenta que suplanta al Banco de Chile

Alerta de seguridad cibernética	8FFR23-01513-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 agosto, 2023
Última revisión	31 agosto, 2023

Indicadores de compromiso

URL sitio falso

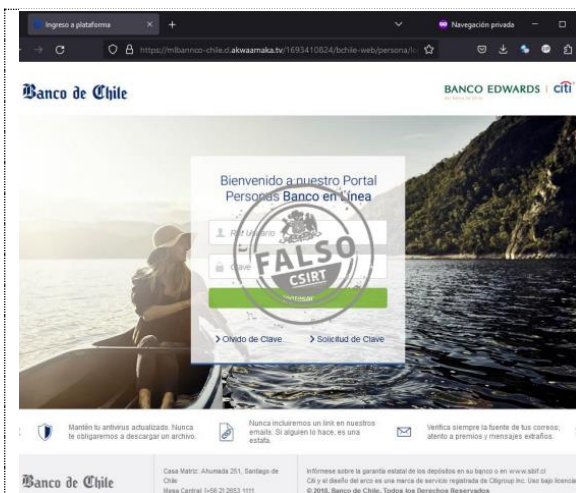
<https://mlbannco-chile.cl.akwaamaka.tv/1693410824/bchile-web/persona/login/index.html/login>

Dirección IP

[68.66.226.75]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01513-01/>



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

Alerta de seguridad cibernética	8FFR23-01514-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 agosto, 2023
Última revisión	31 agosto, 2023

Indicadores de compromiso

URL sitio falso

[https://mlbancochlle.actech.\[.\].pk/1693412118/bchile-web/persona/login/index.html/login](https://mlbancochlle.actech.[.].pk/1693412118/bchile-web/persona/login/index.html/login)

Dirección IP

[103.227.176.26]

Enlace para revisar el informe:

<https://www.csirt.gob.cl/alertas/8ffr23-01514-01/>

CONTACTO Y REDES SOCIALES CSIRT

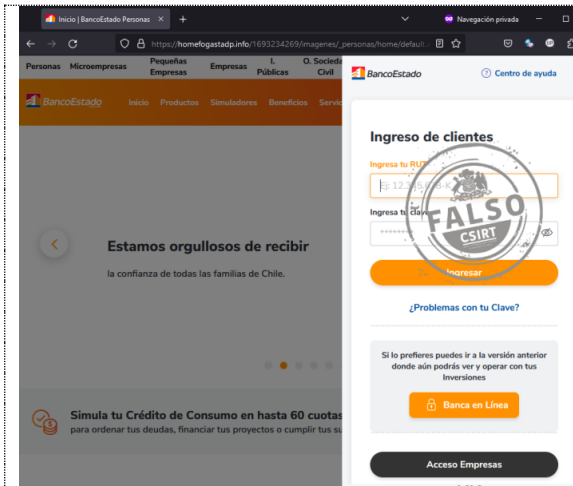
<https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
<https://www.linkedin.com/company/csirt-gob>

Boletín de Seguridad Cibernética N° 217

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

BOLETÍN 13BCS23-00226-01 | Semana del 25 al 31 de agosto de 2023

2. Phishing



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00880-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 agosto, 2023
Última revisión	29 agosto, 2023
URL redirección	N/A
URL redirección	https://senstadolinea[.]info/activacion/cuenta-zuku/
URL sitio falso	https://homefogastadp[.]info/1693234269/imagenes/_personas/home/default.a sp
Dirección IP	[107.190.131.66]
Enlace para revisar loC:	https://www.csirt.gob.cl/alertas/8fph23-00880-01/



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado

Alerta de seguridad cibernética	8FPH23-00881-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 agosto, 2023
Última revisión	30 agosto, 2023
Indicadores de compromiso	
URL redirección	https://senstadolinea[.]info/activacion/cuenta-nqcs/
URL sitio falso	https://homefogastadp[.]info/1693403494/imagenes/_personas/home/default.a sp
Dirección IP sitio falso	[107.190.131.66]
Enlace para revisar loC:	https://www.csirt.gob.cl/alertas/8fph23-00881-01/

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



CSIRT comparte información de vulnerabilidades que afectan algunos productos de Cisco

Alerta de seguridad cibernética	9VSA23-00886-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 agosto, 2023
Última revisión	25 agosto, 2023

CVE		
CVE-2023-20168	CVE-2023-20200	CVE-2023-20234
CVE-2023-20169	CVE-2023-20115	CVE-2023-20230

Fabricante
Cisco

Productos afectados
Cisco NX-OS Software
Switches Cisco Nexus 3000 y 9000 series.
Cisco Firepower 4100 Series, Firepower 9300 Security Appliances y UCS 6300 Series Fabric Interconnects.

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/vulnerabilidades/9VSA23-00886-01/>



CSIRT comparte información de vulnerabilidades parchadas en Google Chrome 116

Alerta de seguridad cibernética	9VSA23-00887-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 agosto, 2023
Última revisión	28 agosto, 2023

CVE	
CVE-2023-4430	CVE-2023-4427
CVE-2023-4429	CVE-2023-4431
CVE-2023-4428	

Fabricante
Google

Productos afectados
Google Chrome 116

Enlaces para revisar el informe:
<https://www.csirt.gob.cl/vulnerabilidades/9VSA23-00887-01/>

CSIRT comparte información de dos vulnerabilidades en VMware Aria Operations for Networks, una crítica

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° 217

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

BOLETÍN 13BCS23-00226-01 | Semana del 25 al 31 de agosto de 2023



INFORME DE Vulnerabilidad

9VSA23-00888-01
CSIRT comparte información de vulnerabilidades en VMware Aria Operations, una de ellas crítica

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



Alerta de seguridad cibernética	9VSA23-00888-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 agosto, 2023
Última revisión	31 agosto, 2023
CVE	
CVE-2023-34039	
CVE-2023-20890	
Fabricante	
VMware	
Productos afectados	
VMware Aria Operations for Networks 6.x	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00888-01/	



INFORME DE Vulnerabilidad

9VSA23-00889-01
CSIRT comparte vulnerabilidades parchadas para Mozilla Firefox 116

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



CSIRT comparte vulnerabilidades nuevas en Mozilla Firefox 116			
Alerta de seguridad cibernética	9VSA23-00889-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Alto		
TLP	Blanco		
Fecha de lanzamiento original	31 agosto, 2023		
Última revisión	31 agosto, 2023		
CVE			
CVE-2023-4573	CVE-2023-4577	CVE-2023-4580	CVE-2023-4583
CVE-2023-4574	CVE-2023-4578	CVE-2023-4581	CVE-2023-4584
CVE-2023-4575	CVE-2023-4579	CVE-2023-4582	CVE-2023-4585
CVE-2023-4576			
Fabricante			
Mozilla			
Productos afectados			
Firefox 116			
Firefox ESR 102.14			
Firefox ESR 115.1			
Thunderbird 102.14			
Thunderbird 115.1.			
Enlaces para revisar el informe:			
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00889-01/			

CONTACTO Y REDES SOCIALES CSIRT

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

4. Noticias y concientización

Nuevas direcciones de correo electrónico del CSIRT de Gobierno

Nuevas direcciones de correo electrónico



A partir de hoy, **miércoles 30 de agosto**, el CSIRT de Gobierno contará con **nuevas cuentas de correo electrónico**, las que reemplazarán las ya existentes. Estos cambios son:



soc@interior.gob.cl será **incidentes@interior.gob.cl**

para notificar incidentes, incluyendo el DS 273, solicitar ayuda técnica o reportar problemas.



legalcsirt@interior.gob.cl será **csirt-legal@interior.gob.cl**

para requerimientos legales o judiciales.



comunicaciones@interior.gob.cl será **csirt-comunicaciones@interior.gob.cl**

para solicitar información de los servicios, capacitaciones, requerimientos para eventos o actividades de ciberseguridad y estadísticas.

Las cuentas de correo electrónico serán eliminadas el día viernes 15 de septiembre, por lo que los invitamos a comenzar desde ya a utilizar las nuevas cuentas.

CONTACTO Y REDES SOCIALES CSIRT

Coordinador Nacional de Ciberseguridad destaca agenda chilena en foro de ciberseguridad de la CEPAL

Para anunciar los avances y desafíos de la Agenda Nacional Pública de Ciberseguridad, el Coordinador Nacional de Ciberseguridad de Chile, Daniel Álvarez, expuso en el Seminario de Ciberseguridad en América Latina y el Caribe, organizado por la Comisión Económica para América Latina y el Caribe de las Naciones Unidas, CEPAL.

En el foro, realizado el pasado 24 de agosto, Daniel Álvarez informó sobre los aspectos que se contemplan en la propuesta de la Política Nacional y el proyecto de Ley Marco; ambos enmarcados en la Agenda Nacional de Ciberseguridad, indicando que “Chile efectivamente ha logrado avanzar en materia de ciberseguridad con una real política de Estado. Llevamos tres gobiernos consecutivos, y la última política nacional de ciberseguridad que se aprobó hace un tiempo por el Comité Ministerial ya está en la Contraloría. Así que esperamos que en unas semanas más se publique y podamos anunciarla”, afirmó Álvarez.

Cabe destacar que dicha política da cuenta de un consenso político, técnico y personal, ya que tal como explicó el experto, “los desafíos que enfrentamos en la actualidad son similares a los de hace unos 5 o 6 años, lo cual indica que el proceso de planificación ha sido el acertado”.

La noticia completa: <https://www.csirt.gob.cl/noticias/cepal-ciberseguridad-2023/>.



El coordinador Nacional de Ciberseguridad, Daniel Álvarez, realizando su exposición.

CONTACTO Y REDES SOCIALES CSIRT

Especialistas del CSIRT participan de ejercicio de ciberseguridad de las FF.AA. Trabún 2023

El Centro Coordinador de CSIRT de Defensa (CCCD) organizó por segundo año consecutivo el Ejercicio Trabún, que tiene como objetivo mejorar la preparación de los equipos de respuesta ante incidentes de ciberseguridad (CSIRT) del Estado y la Defensa Nacional, a través de una competencia entre teams de especialistas elegidos por cada institución.

Con ese objetivo en mente, en Trabún 2023 participaron los CSIRT de Defensa, del Estado Mayor Conjunto (EMCO), del Ejército, la Armada, la Fuerza Aérea y un equipo de las subsecretarías de Defensa y para las Fuerzas Armadas. El equipo que representó al CSIRT del Ministerio del Interior (compuesto por sus analistas Juan Esteban Moraga, Eduardo Riveros y Kevin Anguita) obtuvo el primer lugar este año.

La noticia completa: <https://www.csirt.gob.cl/noticias/csirt-trabun-2023/>.



Premiación de los representantes del CSIRT del Ministerio del Interior.

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>

CISA: Analista del CSIRT participó en workshop de sistemas de control industrial

Entre el 21 y 25 de agosto se llevó a cabo el primer workshop de sistemas de controles industriales, actividad organizada por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), Titanium y Latin America and Caribbean Cyber Competence Centre (LAC4), y que tuvo como objetivo fortalecer e identificar las infraestructuras críticas de los distintos países.

Durante cinco días, los asistentes, provenientes desde 23 países del mundo, entre ellos Brasil, Paraguay, Uruguay, Chile, Jordania, Congo, Sudáfrica y República Dominicana, exploraron componentes críticos de los sistemas de control industrial (ICS), controladores lógicos programables (PLC), sistemas de control de distribución (DSC), controles de supervisión y adquisición de datos (SCADA), terminales remotas (RTU), entre otros dispositivos.





César López, analista de malware del CSIRT de Gobierno y representante de Chile en este encuentro, aseguró que “fue una actividad muy interesante en la que pudimos practicar y aplicar nuestros conocimientos en distintas situaciones y escenarios, además de poder compartir conocimientos y experiencias con personas de distintos países, tanto del sector público como privado”.

La nota completa: <https://www.csirt.gob.cl/noticias/cisa-analista-del-csirt-participo-en-workshop-de-sistemas-de-control-industrial/>



César López recibe un reconocimiento de la CISA.

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 | Contraseñas robustas

Como todo en ciberseguridad, las mejores prácticas al crear claves difíciles de vulnerar por parte de delincuentes cambian y se actualizan a medida que avanza la tecnología y mutan las modalidades de ataque. Por ejemplo, ya no se recomienda cambiar periódicamente de contraseñas. Es por esto que recopilamos algunas de las recomendaciones más importantes al momento de crear nuevas claves, tanto para usuarios como para los encargados de ciberseguridad.

También en formato PDF: <https://www.csirt.gob.cl/recomendaciones/ciberconsejos-contrasenas-2023/>



The infographic is divided into three sections. The top-left section, titled 'CIBERCONSEJOS MEJORES PRÁCTICAS PARA TENER CLAVES ROBUSTAS', features an illustration of a yellow padlock on a purple keyboard key labeled 'LOGIN'. The top-right section, 'Características de las contraseñas', lists six bullet points: minimum length of 8 characters, prohibition of common passwords, allowing but not forcing symbols, no forced periodic changes (with a sub-point that people tend to invent weaker keys), awareness against personal data, and no key reuse. The bottom section, 'Más allá de las contraseñas', recommends Multi-Factor Authentication (MFA) and lists biometrics, location, and patterns as examples, along with the use of password managers.

CIBERCONSEJOS

MEJORES PRÁCTICAS PARA TENER CLAVES ROBUSTAS

Características de las contraseñas





- Largo mínimo: 8 caracteres.
- Prohibir las contraseñas más comunes.
- Permitir, pero NO obligar al uso de símbolos.
- NO forzar el cambio periódico de las contraseñas.
 - Las personas tienden a inventar claves cada vez menos seguras.
- Concienciar contra el uso de datos personales, nombres de familiares o mascotas.
- Enseñar que no se debe repetir claves entre distintas cuentas.

Más allá de las contraseñas

Expertos recomiendan a las organizaciones no basar la autenticación de sus trabajadores únicamente en las claves:

- Implementar mecanismos para la autenticación multi-factor (MFA). Como por ejemplo:
 - Biometría
 - Ubicación
 - Patrones
- Implementar el uso de administradores de contraseñas.





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. 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>

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.

- Krysthel Unda.
- Alexi Contreras.
- Gonzalo Andrés Araya Navarrete.
- Orietta San Martín Runilar.
- Felipe Milacura.
- Ewald Hollstein.
- Franco Valerio.
- Patricio Andrés Allendes Herrera.
- Claudio Andrés Obeid Alarcón.
- Hilario Arturo Cáceres Cousiño.
- Gabriel Torres.
- Juan Henríquez Iturra.
- Jaime Uribe Guzmán.
- Emanuel Alarcón.
- Carlos Fabián Molina.

CONTACTO Y REDES SOCIALES CSIRT