CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 218

semana del 1 al 7 de septiembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

12

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

23

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

60

Las mitigaciones son útiles en productos de Apple, Cacti, Apache y Google.

PARCHES COMPARTIDOS

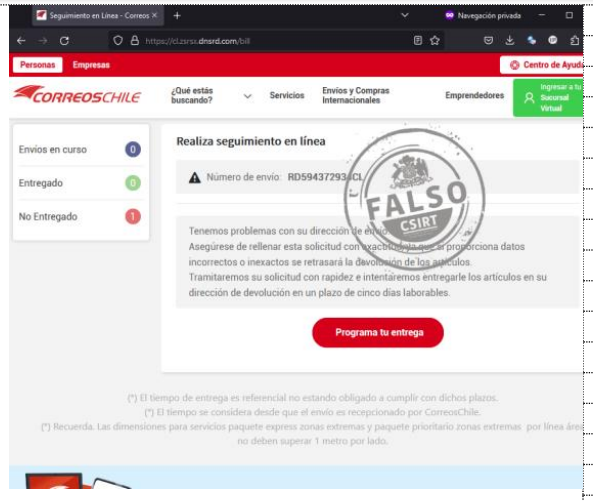
4

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

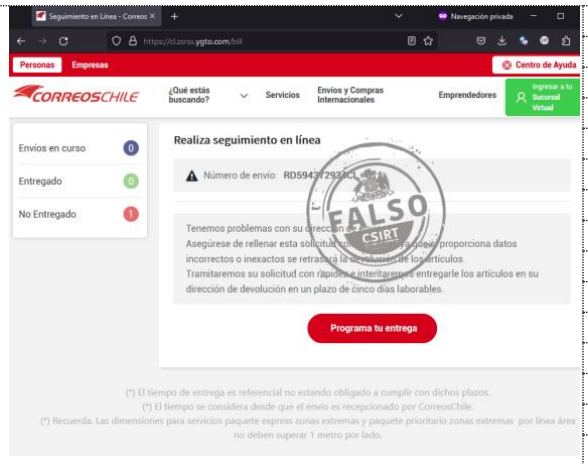
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

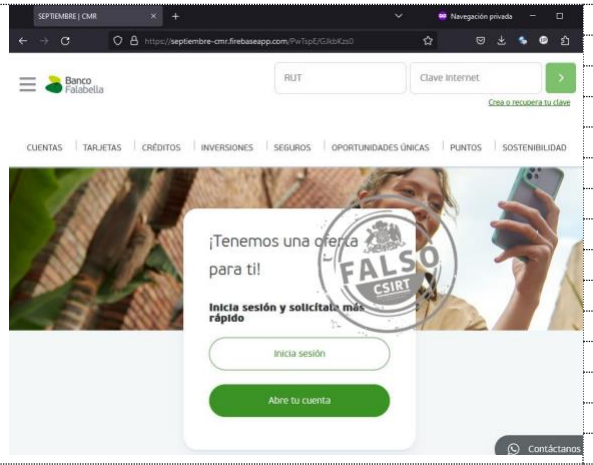
1. Sitios fraudulentos



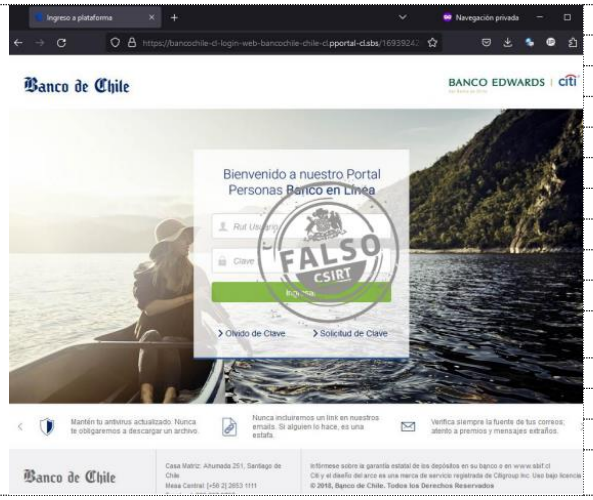
CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01515-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 septiembre, 2023
Última revisión	5 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://cl.zsrsx.dnsrd[.]com/bill	
URL de redirección	
N/A	
IP del sitio falso	
[43.153.106.5]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01515-01/	



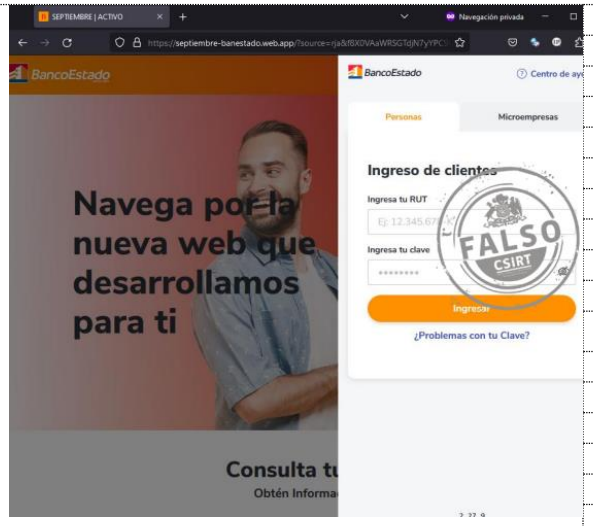
CSIRT alerta de una nueva página fraudulenta que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01516-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 septiembre, 2023
Última revisión	5 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://cl.zsrsx.ygto[.]com/bill	
Dirección IP	
[43.153.106.5]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01516-01/	



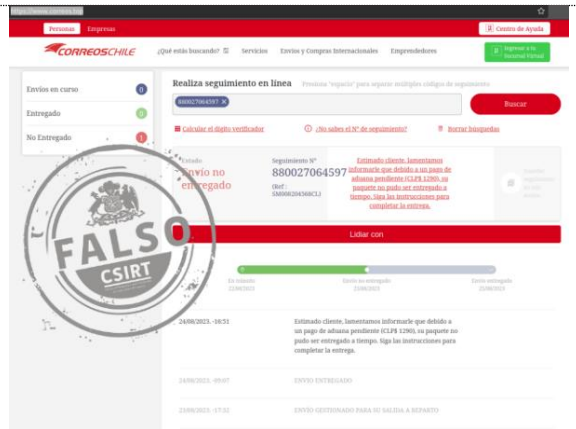
CSIRT alerta de nueva página fraudulenta que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FFR23-01517-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 septiembre, 2023
Última revisión	5 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://septiembre-cmr.firebaseapp[.]com/PwTspE/GJkbKzs0	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01517-01/	



CSIRT alerta de nueva página fraudulenta que suplanta a Banco de Chile	
Alerta de seguridad cibernética	8FFR23-01518-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 septiembre, 2023
Última revisión	5 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://bancochile-cl-login-web-bancochile-chile-cl.pportal-cl.sbs/1693924248/bancochile-web/persona/login/index.html/login	
Dirección IP	
[104.21.50.101]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01518-01/	

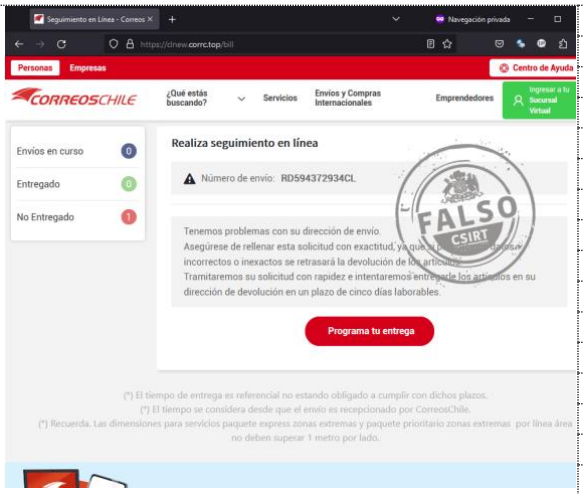


CSIRT alerta de nueva página fraudulenta que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01519-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 septiembre, 2023
Última revisión	6 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://septiembre-banestado.web[.]app/?source=rja&f8X0VAaWRSGTdjN7yYPC9HOBDKqbF3wrIchnEvmU4zMgLJtZk6xi2Qo5lpeu1s	
URL de redirección	
https://bit[.]ly/40wP5AM	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01519-01/	

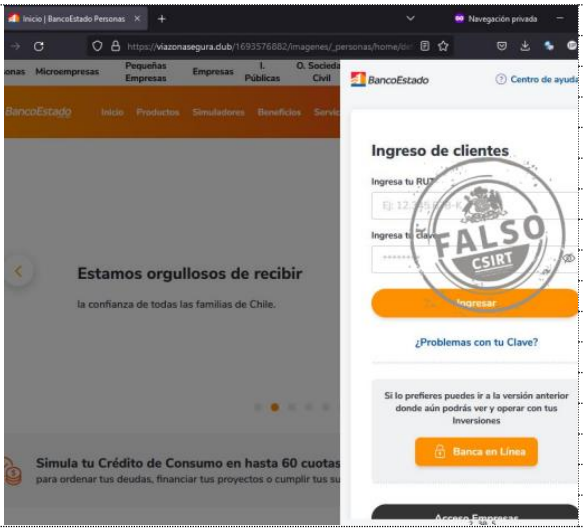


CSIRT alerta de nuevo sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01520-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 septiembre, 2023
Última revisión	7 septiembre, 2023
Indicadores de compromiso	
URL sitio falso	
https://msghub[.]life/correos_cl/	
URL de redirección	
http://gcns[.]me/ZMvItD	
Dirección IP	
[89.147.111.139]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01520-01/	

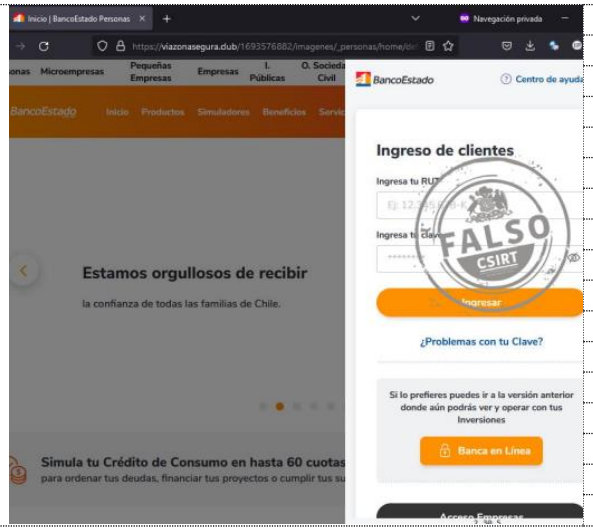
2. Phishing



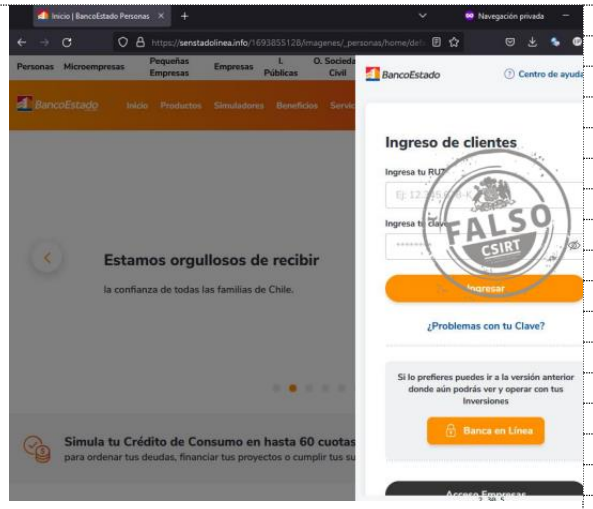
CSIRT alerta de nueva campaña de phishing, que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FPH23-00882-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 septiembre, 2023
Última revisión	1 septiembre, 2023
URL redirección	
N/A	
URL redirección	
https://clnew.corrc[.]top/bill	
URL sitio falso	
https://qrco.de/CorreosChile	
Dirección IP	
[49.51.142.129]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00882-01/	



CSIRT alerta de nueva campaña de phishing, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00883-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 septiembre, 2023
Última revisión	1 septiembre, 2023
Indicadores de compromiso	
URL redirección	
https://senstadolinea[.]info/1693577583/imagenes/_personas/home/default.asp	
URL sitio falso	
https://humanbalance[.]com.co/activacion/cuenta-ukqk/	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00883-01/	

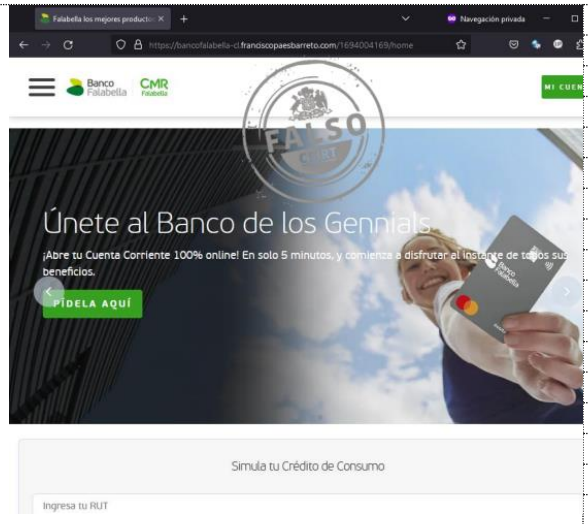


CSIRT alerta de nueva campaña de phishing, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00884-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 septiembre, 2023
Última revisión	1 septiembre, 2023
Indicadores de compromiso	
URL redirección	
https://senstadolinea[.]info/1693577583/imagenes/_personas/home/default.asp	
URL sitio falso	
https://humanbalance[.]com.co/activacion/cuenta-ukqk/	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00884-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00885-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	4 septiembre, 2023
Última revisión	4 septiembre, 2023
Indicadores de compromiso	
URL redirección	
https://senstadolinea[.]info/1693577583/imagenes/_personas/home/default.asp	
URL sitio falso	
https://humanbalance[.]com.co/activacion/cuenta-ukqk/	
Dirección IP sitio falso	
[107.190.131.66]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00885-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FPH23-00886-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 septiembre, 2023
Última revisión	5 septiembre, 2023
Indicadores de compromiso	
URL redirección	
https://www-bancofalabella.cl.chacaquynhnhai[.]vn/1693937868/home	
URL sitio falso	
https://sempel[.]com.br/bancofalabella/cuenta-hvpe/	
Dirección IP sitio falso	
[103.9.157.196]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00886-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a Banco Falabella	
Alerta de seguridad cibernética	8FPH23-00887-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 septiembre, 2023
Última revisión	6 septiembre, 2023
Indicadores de compromiso	
URL redirección	
https://bancofalabella-cl.franciscopaesbarreto[.]com/1694004169/home	
URL sitio falso	
https://sempel[.]com.br/bancofalabella/cuenta-jvzw/	
Dirección IP sitio falso	
[108.167.168.18]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00887-01/	

3. Malware

CSIRT alerta de nueva campaña de phishing con malware Agent Tesla, difundido en falso CV	
Alerta de seguridad cibernética	2CMV23-00428-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 septiembre, 2023
Última revisión	6 septiembre, 2023
Indicadores de compromiso	
URL-Dominio	
https://discordapp.com/api/webhooks/1137023390029459558/ldz8S9vhgT9q0YyJluiWCS8K8CG_TiDgPSszw3j3WD-7RiiwgdrOqropK3lNmkTJqLC6	
SHA256	
819b818549255b76077e9033d8450b6731d43998df92e5f45a7cda660c0bce0eedc17b778240c4aa6910af9803166fc092513782e101df115048c545683dce66	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00428-01/	

CSIRT alerta de campaña de phishing con malware Mekotio, difundida en email que suplanta al SII	
Alerta de seguridad cibernética	2CMV23-00429-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 septiembre, 2023
Última revisión	6 septiembre, 2023
Indicadores de compromiso	
URL-Dominio	
https://www.stivsolutions[.]com/factsiimarzonopagada/verfact/?hash={mail} https://www.stivsolutions[.]com/factsiimarzonopagada/	
SHA256	
65dd04ec6ea0baf56b2ef31e170c826d7f10797be56f13c476bf669b4419c75b6f1322c3e2a7869f0ff396a0b6d8df069a61af4b04fa65b924bab9fab1aa843f	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00429-01/	

4. Vulnerabilidades

CSIRT comparte vulnerabilidades contenidas en el Boletín de Seguridad de Android Septiembre 2023	
Alerta de seguridad cibernética	9VSA23-00890-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 septiembre, 2023
Última revisión	6 septiembre, 2023

CVE

CVE-2023-35669	CVE-2023-35667	CVE-2023-33021
CVE-2023-35674	CVE-2023-35670	CVE-2023-28581
CVE-2023-35675	CVE-2023-35682	CVE-2022-40534
CVE-2023-35676	CVE-2023-35684	CVE-2023-21646
CVE-2023-35687	CVE-2023-35664	CVE-2023-21653
CVE-2023-35679	CVE-2023-35671	CVE-2023-28538
CVE-2023-35658	CVE-2023-35680	CVE-2023-28549
CVE-2023-35673	CVE-2023-35683	CVE-2023-28573
CVE-2023-35681	CVE-2023-35677	CVE-2023-33015
CVE-2023-35665	CVE-2023-28584	CVE-2023-33016
CVE-2023-35666	CVE-2023-33019	

Fabricante

Google

Productos afectados

Android

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00890-01/

CSIRT comparte vulnerabilidades parchadas en nueva actualización semanal de seguridad de Google Chrome 116	
Alerta de seguridad cibernética	9VSA23-00891-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 septiembre, 2023
Última revisión	6 septiembre, 2023

CVE

CVE-2023-4761	CVE-2023-4763
CVE-2023-4762	CVE-2023-4764

Fabricante

Google

Productos afectados

Google Chrome 116

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00891-01/

CSIRT comparte información de vulnerabilidades parchadas en Apache SuperSet 2.1.1	
Alerta de seguridad cibernética	9VSA23-00892-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 septiembre, 2023
Última revisión	7 septiembre, 2023
CVE	
CVE-2023-39265	CVE-2023-36388
CVE-2023-37941	CVE-2023-30776
Fabricante	
Apache	
Productos afectados	
Apache SuperSet	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00892-01/	

CSIRT comparte información de vulnerabilidades parchadas en Cacti 1.2.25	
Alerta de seguridad cibernética	9VSA23-00893-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 septiembre, 2023
Última revisión	7 septiembre, 2023
CVE	
CVE-2023-30534	
CVE-2023-39360	
CVE-2023-39361	
CVE-2023-39357	
CVE-2023-39362	
CVE-2023-39359	
CVE-2023-39358	
CVE-2023-39365	
CVE-2023-39364	
CVE-2023-39366	
CVE-2023-39510	
CVE-2023-39511	
CVE-2023-39512	
CVE-2023-39513	
CVE-2023-39514	
CVE-2023-39515	
CVE-2023-39516	
CVE-2023-31132	
Fabricante	
Cacti	
Productos afectados	
Cacti, versiones anteriores a la 1.2.25	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00893-01/	

CSIRT alerta de dos vulnerabilidades día cero parchadas por Apple	
Alerta de seguridad cibernética	9VSA23-00894-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 septiembre, 2023
Última revisión	7 septiembre, 2023
CVE	
CVE-2023-41064 CVE-2023-41061	
Fabricante	
Apple	
Productos afectados	
iOS anterior a 16.6.1. iPadOS anterior a 16.6.1. macOS Ventura anterior a 13.5.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00894-01/	

5. Noticias y concientización

Cristian Bravo, jefe del CSIRT: "Con la nueva política nacional de ciberseguridad, no estamos cuidando máquinas, estamos cuidando personas"

El jefe del CSIRT de Gobierno, Cristian Bravo, fue entrevistado sobre la segunda versión de la Política Nacional de Ciberseguridad en el más reciente capítulo de TrendTIC Podcast.

En el programa, Bravo destacó que se presentó una propuesta de la segunda versión de la Política Nacional de Ciberseguridad, la cual consiste en una "actualización y una continuidad de los puntos más importantes de la primera versión. Si bien la Política 2023-2028 también tiene cinco pilares, la nueva propuesta se enfoca en una preocupación particular y primordial por las personas, y ahí el slogan que hemos acuñado: no estamos cuidando máquinas, estamos cuidando personas".

Pueden encontrar un resumen de lo hablado aquí, y el video completo de la entrevista, aquí: https://www.csirt.gob.cl/noticias/entrevista-cristian-bravo/

Delegaciones de Colombia y EE.UU. visitaron las dependencias del CSIRT

Como parte de una iniciativa de fortalecimiento de la colaboración entre fuerzas armadas amigas, el Estado Mayor Conjunto de la Defensa Nacional invitó a Chile durante agosto a responsables de ciberseguridad del Departamento Militar de Texas, Estados Unidos, y del Comando Conjunto Cibernético de Colombia.

Y aprovechando su visita, también conocieron las instalaciones del CSIRT del Ministerio del Interior, donde pudimos mostrarles un poco de nuestro trabajo, aprender cómo realizan ellos su labor, y cómo funciona en ambos casos la vinculación entre los CSIRT y CERT civiles y militares.

La noticia está también disponible aquí: https://www.csirt.gob.cl/noticias/visitas-colombia-y-ee-uu/.

Ciberconsejos | Importancia de capacitar a los equipos en las organizaciones

De acuerdo a un informe de noviembre de 2022 de Verizon, «el 85% de las infracciones de ciberseguridad es provocado por errores humanos». Esta cifra tan alta nos demuestra la importancia de capacitar a todos los trabajadores en las organizaciones, para así disminuir los riesgos de que un ciberataque se concrete.

A continuación, te dejamos los siguientes ciberconsejos sobre algunos puntos que definitivamente los trabajadores de una organización deberían conocer.

También los pueden ver aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-contrasenas-2023/.

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.

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.

- David Angelo Zárate Contreras.
- Constanza Nicole Salvo Mattheos.
- Novita.
- Krysthel Unda.
- Jaime Uribe Guzmán.
- Francisco Flefil.
- Felipe Cortés.
- Nicolás Contador.
- Sugy Nam.
- Alexi Contreras Vera.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.08 16:52:07 -03'00'