Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

05-08-2022 | Año 4 | N°161

Boletín de Seguridad Cibernética

Semana del 29 de julio al 4 de agosto de 2022

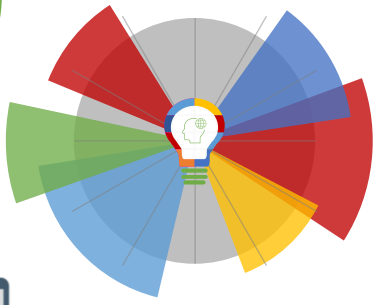
La semana en cifras

Parches

47

para vulnerabilidades

Las mitigaciones son útiles en productos de SonicWall y Red Hat.



IP

1

Informadas

Listado de IP advertidas en múltiples campañas de phishing y de malware.

Se advirtieron

5

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

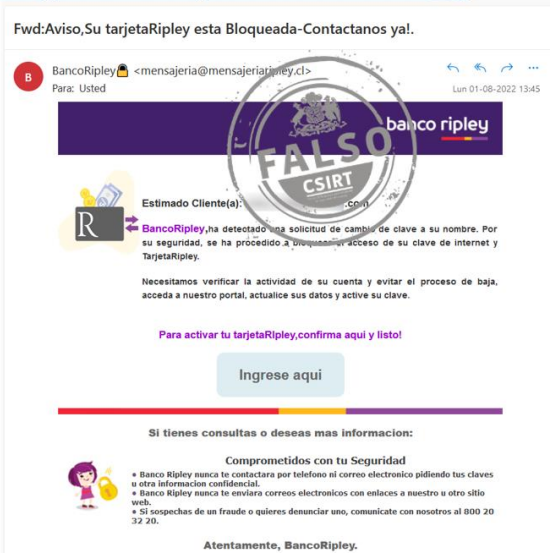
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Phishing 2
Vulnerabilidades 3
Actualidad 5
Muro de la Fama 8

Phishing

Imagen del mensaje



CSIRT advierte phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00568-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de agosto de 2022
Última revisión	2 de agosto de 2022
Indicadores de compromiso	
URL sitio redirección	
https://bit[.]ly/3cv2yoO?l=www.bancoripley.cl http://brombalplatform[.]com/SuiteCRM/XTemplate/enviar02.php?l=1810304182 https://bit[.]ly/3zeNCTu?l=www.bancoripley.cl https://mbmhomeimprovements.com[.]au/activacion/cuenta-tlot/	
URL sitio falso	
https://web.bancoripley.cl.index9[.]com/1659379845/login	
IP	
[207.55.244.15]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00568-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00568-01.pdf	

Vulnerabilidades

CSIRT alerta ante vulnerabilidad crítica en Atlassian Confluence	
Alerta de seguridad cibernética	9VSA22-00682-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de agosto de 2022
Última revisión	1 de agosto de 2022
CVE	
CVE-2022-26138	
Fabricantes	
Atlassian	
Productos afectados	
Questions for Confluence	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00682-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00682-01.pdf	

CSIRT alerta de vulnerabilidades en Android		
Alerta de seguridad cibernética	9VSA22-00683-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	2 de agosto de 2022	
Última revisión	2 de agosto de 2022	
CVE		
CVE-2021-39696	CVE-2022-20344	CVE-2022-20357
CVE-2021-0698	CVE-2022-20345	CVE-2022-20358
CVE-2021-0887	CVE-2022-20346	CVE-2022-20360
CVE-2021-0891	CVE-2022-20347	CVE-2022-20361
CVE-2021-0946	CVE-2022-20348	CVE-2022-22059
CVE-2021-0947	CVE-2022-20349	CVE-2022-22061
CVE-2021-30259	CVE-2022-20350	CVE-2022-22062
CVE-2021-39815	CVE-2022-20352	CVE-2022-22067
CVE-2022-1786	CVE-2022-20353	CVE-2022-22069
CVE-2022-20082	CVE-2022-20354	CVE-2022-22070
CVE-2022-20122	CVE-2022-20355	CVE-2022-22080
CVE-2022-20239	CVE-2022-20356	CVE-2022-25668
Fabricantes		
Google		
Productos afectados		
Android, versiones anteriores a 12 y 12L		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00683-01/		
https://www.csirt.gob.cl/media/2022/08/9VSA22-00683-01.pdf		

CSIRT alerta de vulnerabilidades en productos VMware		
Alerta de seguridad cibernética	9VSA22-00684-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	2 de agosto de 2022	
Última revisión	2 de agosto de 2022	
CVE		
CVE-2022-31656 CVE-2022-31657 CVE-2022-31658 CVE-2022-31659	CVE-2022-31660 CVE-2022-31661 CVE-2022-31662	CVE-2022-31663 CVE-2022-31664 CVE-2022-31665
Fabricantes		
Google		
Productos afectados		
VMware Workspace ONE Access (Access) VMware Workspace ONE Access Connector (Access Connector) VMware Identity Manager (vIDM) VMware Identity Manager Connector (vIDM Connector) VMware vRealize Automation (vRA) VMware Cloud Foundation vRealize Suite Lifecycle Manager		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00684-01/		
https://www.csirt.gob.cl/media/2022/08/9VSA22-00684-01.pdf		

Actualidad

Ciberconsejos para evitar las "fake news"

Las mentiras no son nada nuevo, por supuesto. Pero en la actual Era de la Información, se difunden con una velocidad y amplitud nunca antes vistas. Por esto es clave que sepamos identificar cuando estamos en presencia de las denominadas «fake news», información falsa difundida con el propósito de engañar a la gente y obtener réditos con ello.

Revisa la guía completa aquí: https://www.csirt.gob.cl/recomendaciones/fake-news-2022/

Guía de Mediación Parental 2022

En el marco del mes del niño, la Subsecretaría del Interior, la Fundación Katy Summer y Entel, lanzamos una pauta renovada de consejos para padres y tutores, con el objetivo de educar a los niños, niñas y jóvenes y acompañarlos en su navegación por internet para enfrentar las ciberamenazas. Este año incorporamos las instrucciones prácticas elaboradas por la Fundación Katy Summer sobre cómo elaborar un conversatorio en familia para que los menores de edad puedan contar sus preocupaciones en confianza. Encuéntralo aquí: csirt.gob.cl/media/2022/08/Ciber-Guia-Mediacio%CC%81n-Parental.pdf

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 los sitios web que se ingresen sean los oficiales.

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.

- Alonso Olivares Chevesich
- Hanz Sandoval
- Jair Palma
- Charly Esteban Suárez Ocares
- Jerson Andrés Valenzuela Campusano

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.05 15:27:22 -04'00'