Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

02-09-2022 | Año 4 | N°165

Boletín de Seguridad Cibernética

Semana del 26 de agosto al 1 de septiembre de 2022

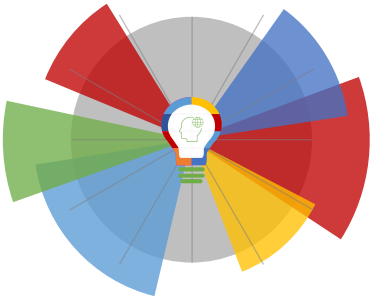
La semana en cifras

Parches

22

para vulnerabilidades

Las mitigaciones son útiles en productos de Google Chrome, Atlassian y Wordpress.



Hash

12

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware

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

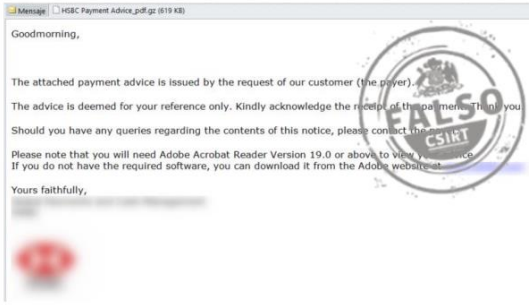
Contenido

Malware

Imagen del mensaje

CSIRT alerta campaña de phishing con falso documento de pago	
Alerta de seguridad cibernética	2CMV22-00334-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de agosto de 2022
Última revisión	29 de agosto de 2022
Indicadores de compromiso	
Asunto	
RE: Pago del saldo	
Correo de salida	
atencionclientes@bufeteaduaneroisa.com	
SHA256	
Nombre: Pago del saldo.zip SHA256: c91e6143bb50eae57133a7404a48eb957527c120d9174fa88a5a5dcd84fc5ed8 Nombre: Pago del saldo.exe SHA256: f2ce0baac026b88699e4d88c97f8f08753f32774541c41094c45d5769c099ed8	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00334-01/	
https://www.csirt.gob.cl/media/2022/08/2CMV22-00334-PH-01.pdf	

Imagen del Mensaje



CSIRT alerta campaña de phishing con falso documento de pago	
Alerta de seguridad cibernética	2CMV22-00335-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de agosto de 2022
Última revisión	29 de agosto de 2022
Indicadores de compromiso	
Asunto	
RE: Pago del saldo	
Correo de Salida	
atencionclientes@bufeteaduaneroisa.com	
SHA256	
Nombre: HSBC Payment Advice_pdf.gz SHA256: 99596b48616c9f3f97ed542537f1c5bde245901878a232a9ef9a56255e796c3c	

Nombre: HSBC Payment Advice_pdf.exe SHA256: bf4efd22ca4470ea82653fb2cd1483acd1951afb1b0ef4988513640ec1c71d66
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00335-01/
https://www.csirt.gob.cl/media/2022/08/2CMV22-00335-PH-01.pdf

Imagen del mensaje

CSIRT alerta ante campaña de phishing con falso documento de pago	
Alerta de seguridad cibernética	2CMV22-00336-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2021
Última revisión	31 de agosto de 2021
Indicadores de compromiso	
Asunto	
RE: Pago del saldo	
Correo de Salida	
atencionclientes@bufeteaduaneroisa.com	
SHA256	
Nombre: Factură de plată.tgz SHA256: c0a8fe7b7aa8f16cfd2078c8b525f0ed11c3ebc7add37c931998c355cbaf06b4 Nombre: Factură de plată.exe SHA256: a540191cd58dafae37a704c4e602b869d0bf09e96d2015de6a30e7d01a1ad0a8 Nombre: progzone.exe SHA256: 83a681fae6f2c3ec5896d2772f43af04a9f7116db74a7082f8c0ab19ca558d43	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00336-01/	
https://www.csirt.gob.cl/media/2022/08/2CMV22-00336-PH-01.pdf	

CSIRT alerta ante campaña de phishing con falso documento de pago	
Alerta de seguridad cibernética	2CMV22-00337-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2021
Última revisión	31 de agosto de 2021
Indicadores de compromiso	
Asunto	
Commande en retrait «Casablanca – Maroc»	
Correo de Salida	
han.hal@shannonbruins.com	
SHA256	
Nombre: INDUSAIR INVOICE T25_REX.7z SHA256: c81a5fc98250b0d1653613e27ea03196ac6872630164d5036405e4abc1e77166 Nombre: MSA, a.s., Hlucinska 641, 747 22 Dolni Benesov, Casablanca.js SHA256: 264d299a0fe5adfa13d59156d2c5c39a6646ee96bfa61cbc4a7ef1c7cdd5d44c Nombre: NBXCJHDSD.exe SHA256: b47cf0eaed7e3798e77eaf01aac5783f2c03f7db7802a5215523d4ccdc631bc5	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00337-01/	
https://www.csirt.gob.cl/media/2022/08/2CMV22-00337-PH-01.pdf	

CSIRT alerta ante nueva campaña de phishing con malware	
Alerta de seguridad cibernética	2CMV22-00338-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de septiembre de 2022
Última revisión	1 de septiembre de 2022
Indicadores de compromiso	
Asunto	
m/v da tong yun agency appointment for discharging operations	
Correo de Salida	
liuhs@coscol.com.cn	
SHA256	

Nombre: VQ88.rar SHA256: d25d246eb950831272291e835d3d9cba00e65800385fbc9f2418577e76eb01d2 Nombre: VQ88.exe SHA256: c18fa2c004bcb50d1d52013a1b96af882e0dec4f4a2b8372015cb624b3951ad3
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00338-01/
https://www.csirt.gob.cl/media/2022/09/2CMV22-00331-PH-01-1.pdf

Vulnerabilidades

CSIRT comparte vulnerabilidad crítica en Bitbucket de Atlassian	
Alerta de seguridad cibernética	9VSA22-00697-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de agosto de 2022
Última revisión	30 de agosto de 2022
CVE	
CVE-2022-36804	
Fabricantes	
Atlassian	
Productos afectados	
Bitbucket Server and Data Center 7.0.0 y posteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00697-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00697-01.pdf	

CSIRT comparte vulnerabilidades en WordPress CMS	
Alerta de seguridad cibernética	9VSA22-00698-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2022
Última revisión	31 de agosto de 2022
CVE	
CVE-pendiente CVE-pendiente CVE-pendiente	
Fabricantes	
Wordpress	
Productos afectados	
WordPress Content Management System (CMS), versiones anteriores a la 6.0.2 (la versión 6.0.2 parcha las vulnerabilidades contenidas en este documento).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00698-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00698-01.pdf	

CSIRT comparte vulnerabilidad grave en Cisco Secure Web Appliance	
Alerta de seguridad cibernética	9VSA22-00699-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de agosto de 2022
Última revisión	31 de agosto de 2022
CVE	
CVE-2022-3038	CVE-2022-3047
CVE-2022-3039	CVE-2022-3048
CVE-2022-3040	CVE-2022-3049
CVE-2022-3041	CVE-2022-3050
CVE-2022-3042	CVE-2022-3051
CVE-2022-3043	CVE-2022-3052
CVE-2022-3044	CVE-2022-3053
CVE-2022-3045	CVE-2022-3054
CVE-2022-3046	CVE-2022-3055
Fabricantes	
Google	
Productos afectados	
Google Chrome anteriores a la versión 105	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00699-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00699-01.pdf	

Actualidad

ALERTA DE SEGURIDAD CIBERNÉTICA: INCIDENTE EN SERVICIO PÚBLICO

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, informó sobre un incidente de seguridad cibernética en un servicio del gobierno, descubierto durante la jornada del jueves 25 de agosto, el cual interrumpió el funcionamiento de sus sistemas y servicios en línea.

El comunicado publicado por el CSIRT de Gobierno ante este incidente puede ser visto aquí: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-incidente-en-servicio-publico/

Ciberconsejos en el Día Mundial del Gamer

El 2008 se estableció el Día Mundial del Gamer por parte de las principales revistas especializadas en videojuegos, por eso hoy en los ciberconsejos del CSIRT de Gobierno explicamos qué es un gamer y entregamos algunos consejos para jugar más seguro. Puedes descargar la campaña completa de cinco imágenes en JPG y PDF aquí: csirt.gob.cl/recomendaciones/ciberconsejos-en-el-dia-mundial-del-gamer/

Ciberconsejos para descargar apps seguras

Si bien las aplicaciones o juegos para los smartphones pueden ser muy útiles o entretenidas, hoy debemos tener mucho cuidado al descargarlas, ya que algunas son creadas con fines maliciosos, como espionaje, acoso o suplantación de identidad. Puedes descargar la campaña completa de cinco imágenes en JPG y PDF aquí: csirt.gob.cl/recomendaciones/ciberconsejos-en-el-dia-mundial-del-gamer/

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.

- Macarena Cristina Alliende Serra
- Erika Cartagena Cartagena
- Milca Elizabeth Acevedo Ormeño