Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

09-12-2021 | Año 3 | N°127

Boletín de Seguridad Cibernética

Semana del 3 al 9 de diciembre de 2021

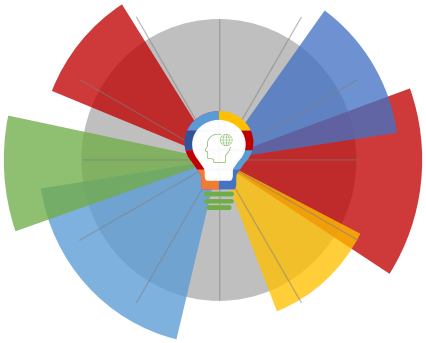
La semana en cifras

Hash

4

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

4

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

45

para vulnerabilidades

Las mitigaciones son útiles en productos IBM, Google y SonicWall.

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

Contenido

Malware

CSIRT informa campaña con malware Emotet	
Alerta de seguridad cibernética	2CMV21-00255-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de diciembre de 2021
Última revisión	06 de diciembre de 2021
Indicadores de compromiso	
SHA256	
5D0311243534A50B4FFFA6BB32A952F86E51194D372741B30DBEA12C51EB4C443D46D69A3CB137E443329C73E8551DCFAA471BC271D891703850A0C931FAACD8	
IoC red	
http://www.duoyuhudong[.]cn/wp-content/we8xi/ http://sadabahar.com[.]np/wp-includes/pUMqITCt83a/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00255-01/	
https://www.csirt.gob.cl/media/2021/12/2CMV21-00255-01-2.pdf	

CSIRT advierte campaña de malware con Emotet	
Alerta de seguridad cibernética	2CMV21-00256-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de diciembre de 2021
Última revisión	9 de diciembre de 2021
Indicadores de compromiso	
SHA256	
cb836996444ea64cbbc74d40ae7a98f45a0ba279176f9b453ab7bcf62a144ded67784b75c77762be449b4a271f9afa04520817197749c84a82ca8d1942867163	
IoC Red	
www.kjtaxpro[.]com/r0bh/ http://173.232.204.89/bnikg[.]exe	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00256-01/	
https://www.csirt.gob.cl/media/2021/12/2CMV21-00256-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en IBM QRadar SIEM	
Alerta de seguridad cibernética	9VSA21-00528-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de diciembre de 2021
Última revisión	6 de diciembre de 2021
CVE	
CVE-2017-15713 CVE-2021-32399 CVE-2021-29650 CVE-2021-29154 CVE-2021-22555 CVE-2020-27777 CVE-2021-3715 CVE-2019-9924 CVE-2018-18751 CVE-2018-11768 CVE-2020-7226 CVE-2020-9492 CVE-2018-8029 CVE-2020-13954 CVE-2021-22696 CVE-2021-28163 CVE-2021-28169 CVE-2021-28165 CVE-2021-29425 CVE-2021-2161	
Fabricante	
IBM	
Productos afectados	
IBM Qradar SIEM: 7.3.0 a 7.4.3 Fix Pack 2, 7.4.3 GA.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00528-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00528-01.pdf	

CSIRT alerta de vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00529-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de diciembre de 2021
Última revisión	7 de diciembre de 2021
CVE	
CVE-2021-4062 CVE-2021-4068 CVE-2021-4067 CVE-2021-4066 CVE-2021-4065 CVE-2021-4064 CVE-2021-4063 CVE-2021-4061 CVE-2021-4052 CVE-2021-4059 CVE-2021-4058 CVE-2021-4057 CVE-2021-4056 CVE-2021-4055 CVE-2021-4054 CVE-2021-4053	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones 70.0.3538.67 a 96.0.4664.45.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00529-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00529-01.pdf	

CSIRT alerta de vulnerabilidades críticas en VPN de SonicWall	
Alerta de seguridad cibernética	9VSA21-00530-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de diciembre de 2021
Última revisión	9 de diciembre de 2021
CVE	
CVE-2021-20038 CVE-2021-20045 CVE-2021-20043 CVE-2021-20040 CVE-2021-20039 CVE-2021-20041 CVE-2021-20042 CVE-2021-20044 CVE-2021-20045	
Fabricante	
SonicWall	
Productos afectados	
SonicWall SMA 100, SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00530-01/	
https://www.csirt.gob.cl/media/2021/12/9VSA21-00530-01.pdf	

Actualidad

El Control de la Semana | No. 19 Acuerdos de Nivel de Servicio

En su número 19, el Control de la Semana explica de qué se trata un Acuerdo de Nivel de Servicio (SLA), y cómo una institución debe definirlo para obtener las mejores prestaciones de sus proveedores.

Todo lo encontrarán en el siguiente documento descargable:
https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-19/

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob https://www.linkedin.com/company/csirt-gob

Ciberconsejos para un escaneo más seguro de los códigos QR

Los códigos QR son esas cajas que parecen «pixeladas» y que han proliferado en Chile especialmente desde el inicio de la actual pandemia, ya que permiten abrir rápidamente información en los teléfonos de clientes y usuarios en lugar de, por ejemplo, usar cartas físicas en los restoranes.

Pero, no sería Ciberconsejos si no fuéramos a recomendarles tener precaución con esta tecnología. Porque así como un QR puede contener información valiosa y segura, también puede ser aprovechado por inescrupulosos para que descarguemos, sin querer, programas maliciosos, o entremos en sitios falsos. Para evitarlo, debemos ser cuidadosos y seguir estos Ciberconsejos: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-qr/.

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 problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Diego Garcés
- Víctor Cofré
- Soledad Pacheco

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob https://www.linkedin.com/company/csirt-gob