Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

28-01-2022 | Año 4 | N°134

Boletín de Seguridad Cibernética

Semana del 21 al 27 de enero de 2022

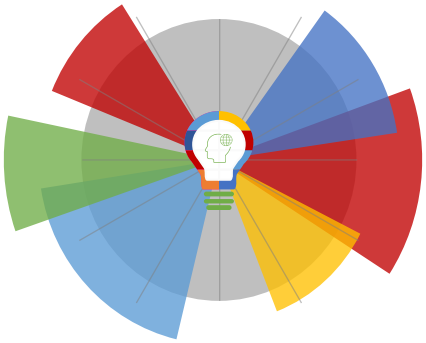
La semana en cifras

Hash

2

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

6

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

22

para vulnerabilidades

Las mitigaciones son útiles en productos Cisco, Red Hat, Apache, Trend Micro, Apple, Polkit,

IP

3

Informadas

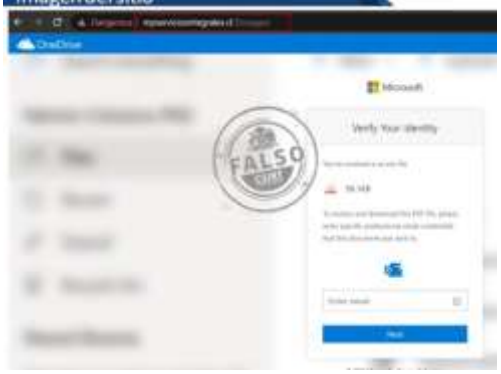
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

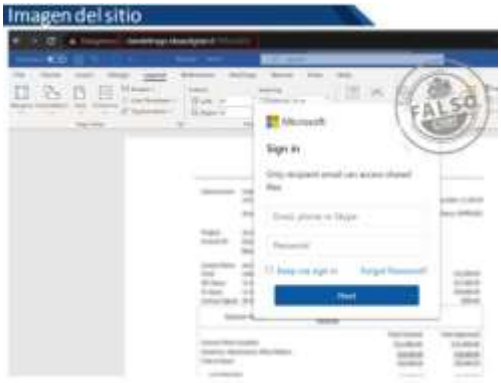
Sitios fraudulentos

Imagen del sitio



CSIRT advierte sitio web que suplanta a plataforma OneDrive	
Alerta de seguridad cibernética	8FFR22-01049-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2022
Última revisión	24 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://mpserviciosintegrales[.]cl/Dosages/	
IP	
[162.241.55.23]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01049-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01049-01.pdf	

Imagen del sitio



CSIRT informa sitio web falso de Microsoft	
Alerta de seguridad cibernética	8FFR22-01050-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2022
Última revisión	25 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://clandeltrago.ideasdigital[.]cl/Office365/	
IP	
[45.228.210.216]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01050-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01050-01.pdf	

Phishing

CSIRT informa de phishing con concurso falso que proviene del Jumbo	
Alerta de seguridad cibernética	8FPH22-00467-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2022
Última revisión	14 de enero de 2022
Indicadores de compromiso	
URL SMS	
https://bingorge[.]site/jumbo/tb.php?_t=16430592821643059488979	
URL sitio falso	
https://cclqma[.]tw/kDWOih63/jumbo/?_t=1643121216874#1643121220225	
IP	
[104.21.93.137]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00467-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00467-01.pdf	

Malware

CSIRT advierte de una campaña de 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	26 de enero de 2022
Última revisión	26 de enero de 2022
Indicadores de compromiso	
SHA256	
5fbef501e52081fdbe5425b94948cd18c0dea6ec2cbd25090456b8455c5bbf7f 5fbef501e52081fdbe5425b94948cd18c0dea6ec2cbd25090456b8455c5bbf7f	
IoC URL	
hXXp://91.240.118.168/qw/as/se.html hXXp://unifiedpharma[.]com/wp-content/5arxM/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00269-01/	
https://www.csirt.gob.cl/media/2022/01/2CMV22-00269-01-5.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades de Cisco RCM para Cisco StarOS	
Alerta de seguridad cibernética	9VSA22-00556-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2022
Última revisión	21 de enero de 2022
CVE	
CVE-2022-20649 CVE-2022-20648	
Fabricante	
Cisco	
Productos afectados	
Estas vulnerabilidades afectan a Cisco RCM para el software Cisco StarOS.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00556-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00556-01.pdf	

CSIRT comparte vulnerabilidades de Cisco Snort Modbus Denial of Service Vulnerability	
Alerta de seguridad cibernética	9VSA22-00557-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2022
Última revisión	21 de enero de 2022
CVE	
CVE-2022-20685	
Fabricante	
Cisco	
Productos afectados	
Esta vulnerabilidad afecta a todas las versiones del proyecto Snort de código abierto anteriores a la versión 2.9.18 y la versión 3.1.0.100. La vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión vulnerable del software de Cisco: Software de cibervisión Software Firepower Threat Defense (FTD) – Todas las plataformas Software de la serie Meraki MX Esta vulnerabilidad afecta a los siguientes productos de Cisco si ejecutan una versión anterior a la primera versión corregida de Cisco Unified Threat	

Defense (UTD) Snort Intrusion Prevention System (IPS) Engine para Cisco IOS XE Software o Cisco UTD Engine para Cisco IOS XE SD- Software WAN: Enrutadores de servicios integrados (ISR) de la serie 1000 Enrutadores de servicios integrados (ISR) de la serie 4000 Software de borde Catalyst 8000V Plataformas perimetrales de la serie Catalyst 8200 Plataformas perimetrales de la serie Catalyst 8300 Plataformas perimetrales de la serie Catalyst 8500 Plataformas perimetrales de la serie Catalyst 8500L Enrutadores de servicios en la nube 1000V Enrutadores virtuales de servicios integrados (ISRv)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00557-01/
https://www.csirt.gob.cl/media/2022/01/9VSA22-00557-01.pdf

CSIRT informa vulnerabilidades en Red Hat AMQ Streams	
Alerta de seguridad cibernética	9VSA22-00558-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2022
Última revisión	21 de enero de 2022
CVE	
CVE-2021-45105 CVE-2021-38153	
Fabricante	
Red Hat	
Productos afectados	
Corrientes AMQ: 1.6.0, 1.6.2, 1.6.4, 1.6.5	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00558-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00558-01.pdf	

CSIRT comparte vulnerabilidades en Apache ShardingSphere ElasticJob-UI	
Alerta de seguridad cibernética	9VSA22-00559-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2022
Última revisión	21 de enero de 2022
CVE	
CVE-2022-22733	
Fabricante	
Apache	
Productos afectados	
ShardingSphere ElasticJob-UI: 3.0.0, 3.0.0 alfa, 3.0.0 beta, 3.0.0 RC1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00559-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00559-01.pdf	

CSIRT comparte vulnerabilidad en Cisco Webex Meetings	
Alerta de seguridad cibernética	9VSA22-00560-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2022
Última revisión	24 de enero de 2022
CVE	
CVE-2022-20654	
Fabricante	
Cisco	
Productos afectados	
Todas las versiones de Cisco Webex Meetings.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00560-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00560-01.pdf	

CSIRT comparte vulnerabilidad en IBM Security SOAR	
Alerta de seguridad cibernética	9VSA22-00561-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2022
Última revisión	24 de enero de 2022
CVE	
CVE-2021-29785	
Fabricante	
Trend Micro	
Productos afectados	
SOAR de seguridad de IBM: 42.0.7058, 42.1.65, 42.2.29, 42.2.39, 42.2.41, 43, 43.0.7661, 43.0.7662	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00561-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00561-01.pdf	

CSIRT comparte vulnerabilidades en Apple WatchOS	
Alerta de seguridad cibernética	9VSA22-00562-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de enero de 2022
Última revisión	24 de enero de 2022
CVE	
CVE-2022-22584 - CVE-2022-22578 - CVE-2022-22585 CVE-2022-22593 - CVE-2022-22590 - CVE-2022-22592 CVE-2022-22589 - CVE-2022-22594	
Fabricante	
Apple	
Productos afectados	
Sistema operativo del reloj: 8.0 19R346, 8.1 19R570, 8.1.1 19R580, 8.3 19S55	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00562-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00562-01.pdf	

CSIRT comparte vulnerabilidades en Apple Safari	
Alerta de seguridad cibernética	9VSA22-00563-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2022
Última revisión	27 de enero de 2022
CVE	
CVE-2022-22590 CVE-2022-22592 CVE-2022-22589 CVE-2022-22594	
Fabricante	
Apple	
Productos afectados	
Apple Safari: 14.0, 14.0.1, 14.0.2, 14.0.3, 14.0.3-14610.4.3.1.7, 14.0.3-15610.4.3.1.7, 14.1, 14.1 14611.1.21.161.7, 14.1 15611.1.21.161 .7, 14.1.1, 14.1.2, 14.1.2 14611.3.10.1.7, 14.1.2 15611.3.10.1.7, 14.5.1, 15.0, 15.1, 15.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00563-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00563-01.pdf	

CSIRT advierte vulnerabilidad en pkexec de Polkit en distribuciones de Linux	
Alerta de seguridad cibernética	9VSA22-00564-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2022
Última revisión	27 de enero de 2022
CVE	
CVE-2021-4034	
Fabricante	
Polkit	
Productos afectados	
Red Hat Enterprise Linux 6 Red Hat Enterprise Linux 7 Red Hat Enterprise Linux 8 Red Hat Virtualización 4 Cualquier producto de Red Hat compatible con Red Hat Enterprise Linux (incluido RHEL CoreOS). Esto incluye: contenedores de productos que se basan en RHEL y envían el paquete polkit y productos que extraen paquetes del canal RHEL (Red Hat OpenShift Container Platform, Red Hat OpenStack	

Platform, Red Hat Virtualization y otros). Asegúrese de que el paquete RHEL polkit subyacente esté actualizado en estos entornos de productos. Ubuntu 21.10 (Impish Indri) Ubuntu 21.04 (Hirsute Hippo) Ubuntu 20.04 LTS (Focal Fossa) Ubuntu 18.04 LTS (Bionic Beaver) Ubuntu 16.04 ESM (Xenial Xerus) Ubuntu 14.04 ESM (Trusty Tahr) Versiones Debian: 0.105-18+deb9u1 0.105-18+deb9u2 0.105-25 0.105-25+deb10u1 0.105-31 0.105-31+deb11u1 0.105-31.1~deb12u1 0.105-31.1 **Varias distribuciones de Linux han emitido oficialmente parches de seguridad. Se recomienda actualizar la versión de seguridad e informarse con su proveedor o fabricante.**
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00564-01/
https://www.csirt.gob.cl/media/2022/01/9VSA22-00564-01-2.pdf

CSIRT informa vulnerabilidad en Log Analysis, componente Apache Log4j	
Alerta de seguridad cibernética	9VSA22-00565-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de enero de 2022
Última revisión	27 de enero de 2022
CVE	
CVE-2021-44228	
Fabricante	
Apple	
Productos afectados	
Log Analysis: 1.3.5.3, 1.3.6, 1.3.6.1, 1.3.7, 1.3.7.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00565-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00565-01.pdf	

Actualidad

Ciberconsejos para proteger nuestros datos en Internet

El incremento en el uso de Internet y plataformas digitales ha hecho que circule mucha información personal y sensible, siendo, en ocasiones, nosotros mismos quienes la exponemos en internet. El 28 de enero se conmemora el Día Internacional de la Protección de Datos, celebración que nació en Europa y que se ha extendido por diferentes partes del mundo, con el objetivo de que los datos de los clientes y usuarios se utilicen de forma segura, confidencial, responsable e íntegra.

Sin embargo, también las personas tenemos un rol importante en el manejo y protección de la información. ¿Cómo cuidas tu privacidad en línea? ¿Qué tipo de datos publicas? ¿Con quiénes la compartes? El CSIRT de Gobierno preparó algunos consejos que te guiarán sobre qué es recomendable y qué no publicar en Internet: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-proteccion-de-datos/

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.

- Víctor Cofré
- Néstor Rivera
- Guillermo Saavedra
- Cristián Acuña
- Javier Candia
- Ricardo Rojas

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.01.31 09:08:17 -03'00'