Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

07-10-2022 | Año 4 | N°170

Boletín de Seguridad Cibernética

Semana del 30 de septiembre al 06 de octubre de 2022

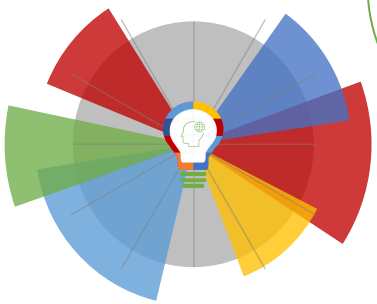
La semana en cifras

Parches

48

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft, Cisco y Atlassian



IP

11

Informadas

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

Se advirtieron

19

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

12

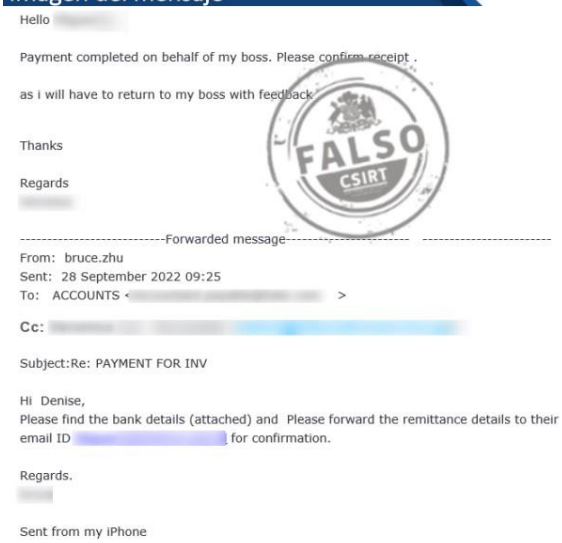
Asociadas a múltiples campañas de phishing con archivos que contienen malware

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

Contenido

Malware

Imagen del mensaje


Hello

Payment completed on behalf of my boss. Please confirm receipt .

as I will have to return to my boss with feedback

Thanks

Regards

FALSO CSIRT

----------Forwarded message----------

From: bruce.zhu
Sent: 28 September 2022 09:25
To: ACCOUNTS <

Cc:

Subject:Re: PAYMENT FOR INV

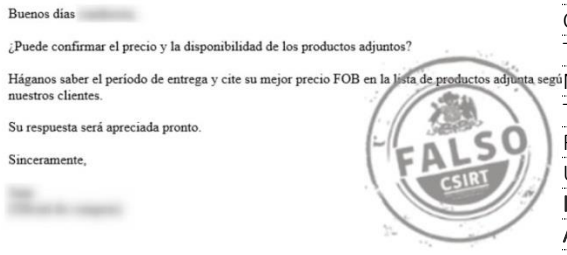
Hi Denise,
Please find the bank details (attached) and Please forward the remittance details to their email ID for confirmation.

Regards.

Sent from my iPhone

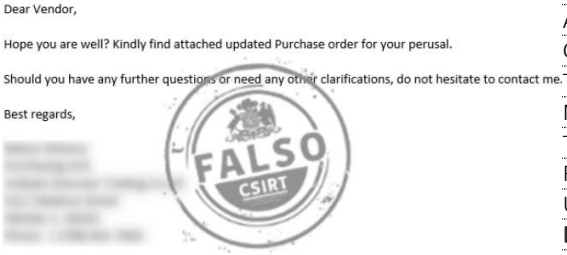
CSIRT alerta ante phishing con malware, con falsa confirmación de pago	
Alerta de seguridad cibernética	2CMV22-00353-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de septiembre de 2022
Última revisión	30 de septiembre de 2022
Indicadores de compromiso	
Asunto	
Ordenar	
Correo de Salida	
info@enertik.ar	
SHA256	
Nombre: Payment copy_00000988.PDF.zip SHA256: 8f3295bfd93ef5affb09b0f2c5ccde4aa33b0c94c117cbfb4b09045fe6201d3e Nombre: Payment copy_00000988.PDF.exe SHA256: 2f33e37286a03dee0a89bbac812d166203e5ddb1f6c2571110a08690a0df1bd0 Nombre: nBFb.exe SHA256: 5ebaba50a78cc3750b1f00750110d368b9522f96939a5d89a5dcc63a346add16	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00353-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00353-01.pdf	

Imagen del mensaje



CSIRT alerta de phishing con falsa solicitud de cotización	
Alerta de seguridad cibernética	2CMV22-00354-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2022
Última revisión	03 de octubre de 2022
Indicadores de compromiso	
Asunto	
Solicitud de cotización	
Correo de Salida	
juanmorales@gmail.com	
SHA256	
Nombre: Solicitud de cotizacion.zip SHA256: def80745672b71f12f1abb6e98c4e4ca8ed86937bd34f6990702162e65814d58 Nombre: Solicitud de cotizacion.exe SHA256: 7a86925eea6d198fb22db8c38502b2cdf4def0f39505d855f66579e2fefa4ce4 Nombre: GISV.exe SHA256: e9d9dbaf6675d4f9ce01ad9dbe355979a4d5f64d1f2237214578e0ebe3e937e7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00354-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00354-01.pdf	

Imagen del mensaje



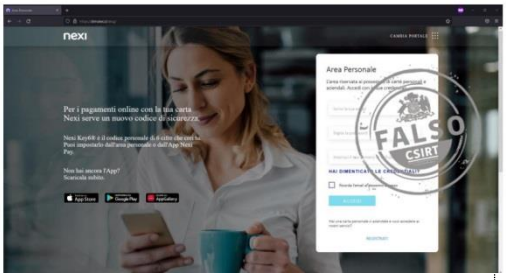
CSIRT alerta de campaña de phishing con malware con falsa orden de compra	
Alerta de seguridad cibernética	2CMV22-00355-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de octubre de 2022
Última revisión	04 de octubre de 2022
Indicadores de compromiso	
Asunto	
Price & Availability	
Correo de Salida	
aal.bou@hkstudyusa.com	
SHA256	
Nombre: Purchase Order-5910G.iso SHA256:	

267db245063e6dd64b6c6d9c911559618d74e8dd20010770f4c59786eeb08c55 Nombre: Purchase Order-5910G.exe SHA256: 0a13141aaefff3f4aaf718c88dca2f3b80a6c8ab555a203437ff1a4b7b50c5c2
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00355-01/
https://www.csirt.gob.cl/media/2022/10/2CMV22-00355-01.pdf

CSIRT alerta phishing que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV22-00356-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de octubre de 2022
Última revisión	06 de octubre de 2022
Indicadores de compromiso	
Asunto	
Fw: Emisión de Boleta de Honorarios Electronica – (891011476516)	
Correo de Salida	
viv@viv.az	
SHA256	
Nombre: 009F7S035531IC4920D.zip SHA256: 445d730300f1f02bab9e7c59ecef59e3fcdaa51ceb499f567adda379006ffea4 Nombre: 009F7S035531IC4920D.msi SHA256: d842c98fb716f9323f7626779ecf4a6140ebd909705f14cfa13c7e834da1260d	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00356-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00356-01-3.pdf	

Sitios fraudulentos

Imagen del sitio



CSIRT alerta de página fraudulenta que suplanta a Nexi	
Alerta de seguridad cibernética	8FFR22-01106-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2022
Última revisión	03 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://dimatec.cl/alog/	
IP	
[200.73.115.31]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01106-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01106-01.pdf	

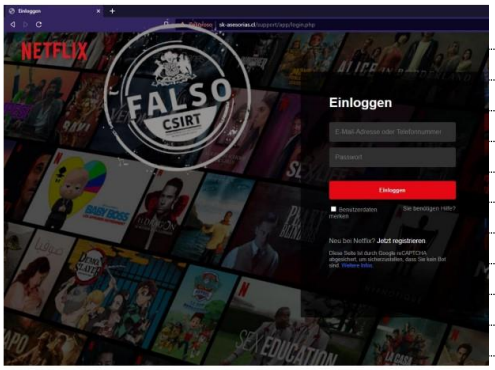
Imagen del sitio

CSIRT alerta de página fraudulenta que suplanta a Outlook Web	
Alerta de seguridad cibernética	8FFR22-01107-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de octubre de 2022
Última revisión	04 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://catalinammdd[.]cl/emptyimages/refresh/index.html	
IP	
[200.73.115.66]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01107-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01107-01.pdf	

Imagen del sitio

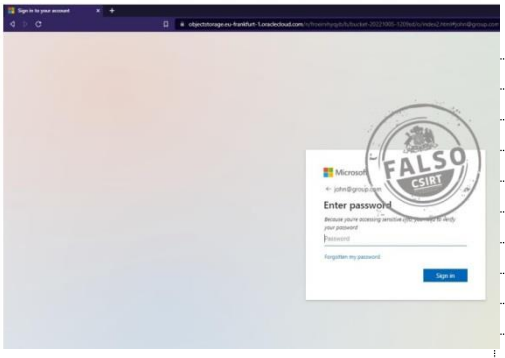
CSIRT alerta ante sitio fraudulento en dominio notebook[.]cl	
Alerta de seguridad cibernética	8FFR22-01102-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de octubre de 2022
Última revisión	05 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
http://notebook[.]cl/tobi.php	
IP	
[104.21.89.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01108-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01108-01.pdf	

Imagen del sitio



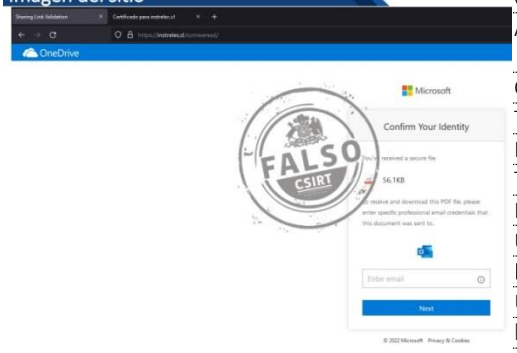
CSIRT alerta ante página fraudulenta que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR22-01109-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de octubre de 2022
Última revisión	05 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://sk-asesorias[.]cl/support/app/login.php	
https://sk-asesorias[.]cl/support/app/	
IP	
[190.3.170.36]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01109-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01109-01-1.pdf	

Imagen del sitio



CSIRT alerta de página que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR22-01110-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de octubre de 2022
Última revisión	05 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://d0ruyoy.marcasocial[.]cl/?D0RuyOY=john@group.com	
https://objectstorage.eu-frankfurt-1.oraclecloud[.]com/n/froeirvhyqyb/b/bucket-20221005-1209sd/o/index2.html#john@group.com	
IP	
[186.64.114.110]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01110-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01110-01.pdf	

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta login de Microsoft	
Alerta de seguridad cibernética	8FFR22-01111-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de octubre de 2022
Última revisión	06 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://instrelec[.]cl/comweresd/	
IP	
[158.69.100.49]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01111-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01111-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta de phishing contra clientes Santander	
Alerta de seguridad cibernética	8FPH22-00607-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de septiembre de 2022
Última revisión	30 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://lati[.]link/dc1m?=app	
https://ajgeotech[.]cl/index/?app=app	
URL sitio falso	
https://harahoritelecomllp[.]com/1664541464/portada/personas/home.asp	
IP	
[173.249.151.122]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00607-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00607-01.pdf	

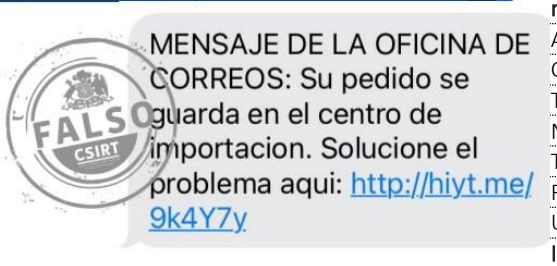
Imagen del mensaje

CSIRT alerta ante campaña de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH22-00608-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2022
Última revisión	03 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://roaccessload[.]click/Web-Client-Upgrade/	
URL sitio falso	
https://roaccessload[.]click/Web-Client-Upgrade/	
IP	
[190.60.225.13]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00608-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00608-01.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing que apunta a clientes Santander	
Alerta de seguridad cibernética	8FPH22-00609-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	04 de octubre de 2022
Última revisión	04 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.skybrands[.]com.np/Recuperalo_Aqui/cuenta-sqft/	
URL sitio falso	
https://santavalpa[.]click/1664891299/portada/personas/home.asp	
IP	
[161.97.66.251]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00609-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00609-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing con mensaje por falso envío retenido	
Alerta de seguridad cibernética	8FPH22-00610-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	06 de octubre de 2022
Última revisión	06 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
http://hiyt[.]me/9k4Y7y	
https://prizegift[.]live/ips_cl/?cep=-AnI4nuDKM9R_nKtqLlc2MdbJPfJcorvK3WDzlOmJ-WqenKPjp-Lunebf0NRJ6FRdOqDHeDMxhVyNEZ25ZHXkE6qsMcmB6jGG72jHsMlN3ex-b4Ix_5d5QpX39qHI18TuhY4xLY8RtoHFSc3lSGf1z2xZbiRJbL07Jab2WOzdMMngR_gwOCnk1lG4qMevPsk94WE1Ig9UG4oy88dhlfXSz9lvuBAwgePB3PweeDZyVuScu2Gbuv3wKwihop62CvF83NRbNb-Ab2InqhSdiG7IUHO6qWyfp_ZHUDU5yvAfwBaFUnrcWi9g9vsmyRe6NlWeFwJ5IgTVifhNPGw03Yp0GMKJGsy2JnMkyJujlAT1Fv1EGvgA-2GJQbKwWpB_O5W&lptoken=16426572061336c818df	
IP	
[5.199.173.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00610-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00610-01.pdf	

Vulnerabilidades

CSIRT alerta ante dos vulnerabilidades zero day en Microsoft Exchange Server	
Alerta de seguridad cibernética	9VSA22-00712-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de septiembre de 2022
Última revisión	30 de septiembre de 2022
CVE	
CVE-2022-41040 CVE-2022-41082	
Fabricantes	
Microsoft	
Productos afectados	
Exchange Server 2013, 2016 y 2019	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00712-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00712-01.pdf	

CSIRT comparte vulnerabilidad crítica en Atlassian Bitbucket Server y Data Center	
Alerta de seguridad cibernética	9VSA22-00713-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de octubre de 2022
Última revisión	03 de octubre de 2022
CVE	
CVE-2022-36804	
Fabricantes	
BIND	
Productos afectados	
Atlassian Bitbucket Server y Data Center	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00713-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00713-01.pdf	

CSIRT alerta ante varias vulnerabilidades en productos Cisco	
Alerta de seguridad cibernética	9VSA22-00714-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	06 de octubre de 2022
Última revisión	06 de octubre de 2022

CVE

CVE-2022-20814 - CVE-2022-20853 - CVE-2022-20929
CVE-2021-27853 - CVE-2021-27854 - CVE-2021-27861
CVE-2021-27862 - CVE-2022-20952 - CVE-2022-20917
CVE-2022-20939 - CVE-2022-20948 - CVE-2022-20686
CVE-2022-20687 - CVE-2022-20688 - CVE-2022-20689
CVE-2022-20690 - CVE-2022-20691 - CVE-2022-20766
CVE-2022-20793 - CVE-2022-20931 - CVE-2022-20728
CVE-2022-20871 - CVE-2022-20775 - CVE-2022-20818
CVE-2022-20769 - CVE-2022-20847 - CVE-2022-20919
CVE-2022-20870 - CVE-2022-20920 - CVE-2022-20769
CVE-2022-20848 - CVE-2022-20915 - CVE-2022-20944
CVE-2022-20855 - CVE-2022-20856 - CVE-2022-20945
CVE-2022-20837 - CVE-2022-20851 - CVE-2022-20930
CVE-2022-20844 - CVE-2022-20864 - CVE-2022-20810
CVE-2022-20850 - CVE-2022-20696

Fabricantes

Cisco

Productos afectados

Cisco IOS XE para switches Cisco Catalyst 9200 Series
Cisco Expressway Series y Cisco TelePresence VCS
Cisco Enterprise NFV Infrastructure Software (NFVIS)
Cisco AsyncOS para Cisco Secure Web Appliance
Cisco SD-WAN Software
Cisco IOS XE Software for Embedded Wireless Controllers on Catalyst 9100 Series Access Point
Cisco Wireless LAN Controller (WLC) AireOS Software
Cisco IOS Software y Cisco IOS XE Software
Cisco IOS XE Software para los switches de las familias Cisco Catalyst 3650, Catalyst 3850 y Catalyst 9000
Cisco IOS XE Software for Embedded Wireless Controllers en Catalyst Access Points
Cisco Catalyst 911 Series Access Points (AP)

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00714-01/
https://www.csirt.gob.cl/media/2022/10/9VSA22-00714-01.pdf

Alerta de Seguridad Cibernética | Vulnerabilidades día cero en Microsoft Exchange Server
Compartimos información sobre dos vulnerabilidades de día cero informadas por Microsoft en sus servidores Exchange en las versiones 2013, 2016 y 2019.
Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00084-01/

ACTUALIZACIÓN. Alerta de Seguridad Cibernética | Vulnerabilidades día cero en Microsoft Exchange Server
Se comparten las recomendaciones de Microsoft para mitigar las vulnerabilidades que afectan al servidor Microsoft Exchange.
Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00084-02/

NUEVA ACTUALIZACIÓN. Alerta de Seguridad Cibernética | Vulnerabilidades día cero en Microsoft Exchange Server
Se comparten nuevas recomendaciones por parte de Microsoft mientras continúan trabajando en un parche.
Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00084-03/

NUEVA MITIGACIÓN. Alerta de Seguridad Cibernética | Vulnerabilidades día cero en Microsoft
Esta alerta comparte una nueva actualización de las recomendaciones entregadas por Microsoft sobre las vulnerabilidades de día cero descubiertas el 30 de septiembre.
Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00084-04/

Exitoso encuentro de los Consejos de Innovación en Ciberseguridad de la OEA en Chile

El miércoles 21 de septiembre se llevó a cabo la tercera reunión anual de los Consejos de Innovación de Ciberseguridad (CIC), evento realizado por la Organización de los Estados Americanos (OEA) junto con el CSIRT de Gobierno de la Subsecretaría del Interior de nuestro país y Cisco Latam.

Los CIC, que ya se han reunido en Chile de manera virtual en 2020 y 2021, han sido un espacio de encuentro para los principales líderes del sector público, privado, la sociedad civil y la academia para impulsar la innovación, concientizar a la ciudadanía y difundir mejores prácticas en materia de ciberseguridad en la región.

Este año el tema central de la reunión fue el desarrollo de la fuerza laboral en ciberseguridad, por lo que tuvo como objetivo abordar el déficit de profesionales en el área de tecnología, seguridad de la información y ciberseguridad en nuestro país, América y el mundo, discutiendo y proponiendo formas de enfrentar esta situación.

La actividad, que convocó a diversos sectores, busca ser un espacio de encuentro para los principales líderes del sector público, privado, la sociedad civil y la academia. Fue así como la reunión fue inaugurada por la ministra de Ciencia, Tecnología, Conocimiento e Innovación, Silvia Díaz; la subsecretaria de Educación Superior, Verónica Figueroa; el rector de la Universidad de Santiago, Rodrigo Vidal; la secretaría del Comité Interamericano contra el Terrorismo (CICTE) de la OEA, Alison Treppel, y el coordinador nacional de Ciberseguridad, Daniel Álvarez.

“El mundo digital está vivo y avanza a una velocidad que la humanidad no alcanza a comprender. Su poder, su funcionamiento en red, su capacidad para concentrar la inteligencia y poder convertirla en algo superior es la mayor promesa y oportunidad para nuestra sociedad, pero conlleva inevitablemente riesgos enormes y difíciles de abordar”, advirtió la ministra Díaz, quien abrió los discursos inaugurales.

Más detalles en el siguiente enlace: https://www.csirt.gob.cl/noticias/cic-chile2022/

Ciberconsejos en el Mes de la Ciberseguridad

El 1 de octubre comenzó el mes de la ciberseguridad, fecha que busca promover la concienciación en ciberseguridad entre la ciudadanía y las organizaciones, a través de la educación y el intercambio de buenas prácticas. En el marco de esta celebración, el CSIRT de Gobierno entrega los siguientes ciberconsejos: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-mes-ciberseguridad/

Ciberdiccionario Volumen 19

En esta ocasión, dos conceptos clave del ejercicio de la ciberseguridad: mitigación y parche, y dos del mundo de las redes sociales y apps de mensajería, doxing y ghosting. También está disponible en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-19/

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.

- Kevin Anguita
- Francisco Vallejo
- Felipe Cortés
- René Lander