Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

30-09-2022 | Año 4 | N°169

Boletín de Seguridad Cibernética

Semana del 23 al 29 de septiembre de 2022

La semana en cifras

Parches

58

para vulnerabilidades

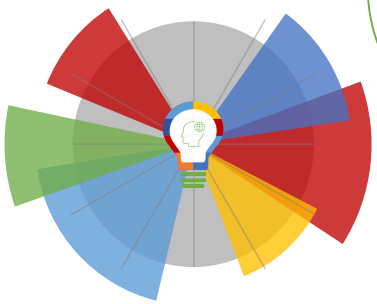
Las mitigaciones son útiles en productos de Google, Meta (WhatsApp), Microsoft, Zoho. Pebble, Sophos e IBM.

IP

11

Informadas

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



Se advirtieron

22

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

10

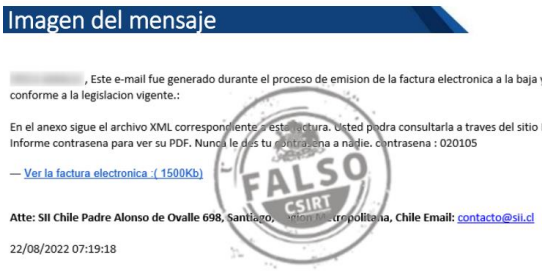
Asociadas a múltiples campañas de phishing con archivos que contienen malware

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

Contenido

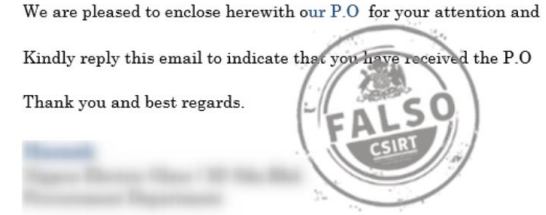
Malware

Imagen del mensaje



CSIRT alerta campaña de phishing que suplanta al SII	
Alerta de seguridad cibernética	2CMV22-00349-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022
Indicadores de compromiso	
Asunto	
✓ FACTURA – ERICA AMALIA , Notificacion Giro Folio 012210001 del 15/08/2022 – SII – – (984837087033)	
Correo de salida	
dukcapiltapinkab@server.tapinkab.go.id	
SHA256	
Nombre: FACTURA-IDSE-34ed1ecf.zip SHA256: cc83ecc8da9069f2e3be95cee116d722163a3d104769711285f10543680849b3 Nombre: FACTURA-IDSE-34ed1ecf-1a2c-4d26-85ba-bc0014sffe5001s4d.msi SHA256: 9fbe66342de53d7ab1c7f3008bb8f5083c4400755903a27947e376da4661692a Nombre: hyr7wehds.exe SHA256: 3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4 Nombre: dns-sd-documento-bajo_____.exe SHA256: 6a27826b490457ccfecebaf98a01325cc1ccecc81917b156aa1e566d141b520c	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00349-01/	
https://www.csirt.gob.cl/edia/2022/09/2CMV22-00349-PH-01.pdf	

Imagen del mensaje



CSIRT alerta de nuevo phishing que suplanta a compañía mexicana	
Alerta de seguridad cibernética	2CMV22-00350-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre de 2022
Indicadores de compromiso	
Asunto	
PO 2209-0651	
Correo de Salida	
kim@merperle.shop	
SHA256	
Nombre: PO 2209-0651.zip SHA256: 1808ff7039d835ecfd81803d6c1f8e6115e63c6df76fc94095d7bb7de1060cda Nombre: PO 2209-0651.exe SHA256: c56318c1a198033aa2b413978062cd8ecc805cac7951551b9cd8be94b3350a3c Nombre: Hsmpqaej.exe SHA256: fa163f94d25970b412b0bbb5a233af3e7d79f63fe843ea3df9052a9cf1902d40	
IoC URL	
https://cdn.discordapp.com/attachments/1022102382827548685/1022696052064796713/Hsmpqaej_Zznxxbyy.png	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00350-01/	
https://www.csirt.gob.cl/media/2022/09/2CMV22-00350-PH-01.pdf	

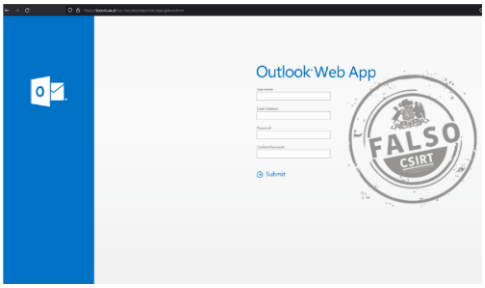
Imagen del mensaje

CSIRT alerta campaña de malware con falsos documentos de pago	
Alerta de seguridad cibernética	2CMV22-00351-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de septiembre de 2022
Última revisión	27 de septiembre de 2022
Indicadores de compromiso	
Asunto	
Re: re: factura proforma	
Correo de Salida	
v.bustos@rsg.cl	
SHA256	
Nombre: RSG USD17309_txt_____.zip	

SHA256: deed64f511e7934edad03d0cbcdf5eb3b9492504f37e8b6e1d054decd61ca278 Nombre: RSG USD17309_txt_____.exe SHA256: 805dba78dbdff90f7f1f8f58b877d2ce89cae2f409db4d7b50eb28bb55a0ac13 Nombre: LBYA.exe SHA256: a341ed5a5e9ba2f7a0a0a5edc9aef870684c6ba26e4e59336ffeec58e835fc2d
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00351-01/
https://www.csirt.gob.cl/media/2022/09/2CMV22-00351-PH-01.pdf

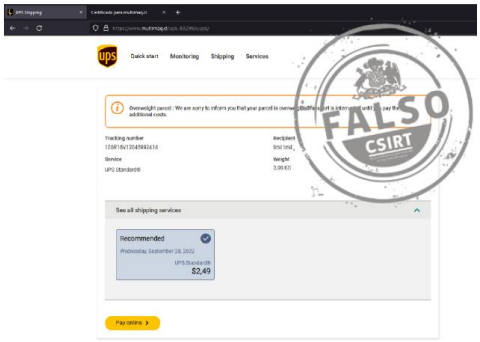
Sitios fraudulentos

Imagen del sitio



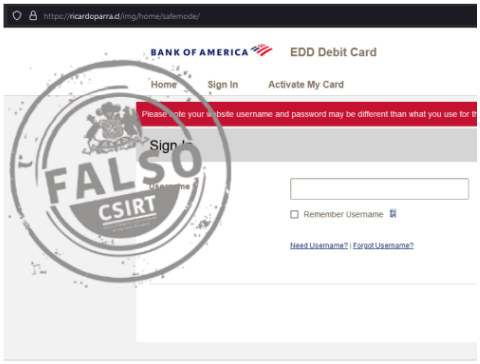
CSIRT alerta de sitio fraudulento que suplanta a Microsoft Outlook	
Alerta de seguridad cibernética	8FFR22-01100-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://tecnoluce[.]cl/wp-includes/seps/mail.seps.gob.ec.html	
IP	
[186.64.118.110]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01100-01/	
https://www.csirt.gob.cl/media/2022/08/8FFR22-01100-01.pdf	

Imagen del sitio



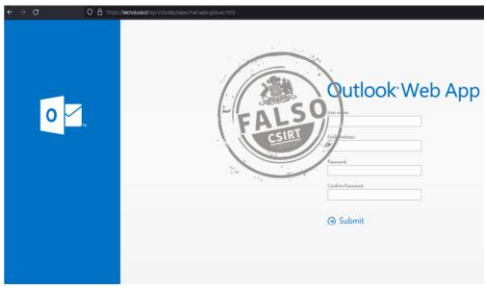
CSIRT alerta ante página fraudulenta que suplanta a UPS	
Alerta de seguridad cibernética	8FFR22-01101-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.multimaq[.]cl/ups-83299/uups/	
IP	
[138.117.148.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01101-01/	
https://www.csirt.gob.cl/media/2022/08/8FFR22-01101-01.pdf	

Imagen del sitio



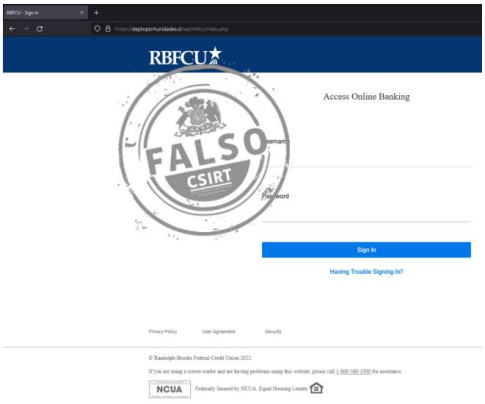
CSIRT alerta de sitio que suplanta al Bank of America	
Alerta de seguridad cibernética	8FFR22-01102-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de septiembre de 2022
Última revisión	28 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://ricardoparra[.]cl/img/home/safemode/ https://ricardoparra[.]cl/config/html http://ricardoparra[.]cl/img/phpscrip/ https://ricardoparra[.]cl/php/form-process/	
IP	
[131.72.236.88]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01102-01/	
https://www.csirt.gob.cl/media/2022/09/8FFR22-01102-01.pdf	

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a Outlook Web	
Alerta de seguridad cibernética	8FFR22-01103-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de septiembre de 2022
Última revisión	28 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://tecnoluce[.]cl/wp-includes/seps/mail.seps.gob.ec.html	
IP	
[186.64.118.110]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01103-01/	
https://www.csirt.gob.cl/media/2022/09/8FFR22-01103-01.pdf	

Imagen del sitio



CSIRT alerta suplantanción de banco RBFCU de EE.UU.	
Alerta de seguridad cibernética	8FFR22-01104-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de septiembre de 2022
Última revisión	29 de septiembre de 2022
Indicadores de compromiso	
URL sitio falso	
https://deptoportunidades[.]cl/wp/rbfcu/index.php	
IP	
[201.217.241.159]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01104-01/	
https://www.csirt.gob.cl/media/2022/09/8FFR22-01104-01.pdf	

Phishing

Imagen del mensaje

CSIRT alerta de nueva campaña de phishing suplantando al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00597-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
http://bit.ly/3S1YUCf https://aplicacion-bancoestado.ga/init?&rpsnv=eac6819d6e578da7ba6eed2a8df7ca3d425246c8 https://aplicacion-bancoestado.ga/init?rpsnv=0b93caee71a9d214d0bbbc5622ea29507e3b8a7a	
URL sitio falso	
https://aplicacion-bancoestado.ga/hipotecarios?25365274diadjhoql6ahl	
IP	
[204.11.58.233]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00597-01/	
https://www.csirt.gob.cl/media/2022/09/8FPH22-00597-01-1.pdf	

Imagen del mensaje

CSIRT alerta campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00598-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://valpa.digitalnoticias.com.mx/activacion/cuenta-tnbl/	
URL sitio falso	
https://nuestro.premiumjp2020.com/1663875740/portada/personas/home.asp	
IP	
[186.64.118.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00598-01/	

https://www.csirt.gob.cl/media/2022/08/8FPH22-00598.01.pdf

Imagen del mensaje

CSIRT alerta por campaña de phishing con falsa alerta de correos pendientes	
Alerta de seguridad cibernética	8FPH22-00599-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
http://w1.nimh.gov.vn/zrr/fx/?email=(correo)	
URL sitio falso	
http://w1.nimh.gov.vn/zrr/fx/?email=(correo)	
IP	
[103.124.92.130]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00599-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00599-01.pdf	

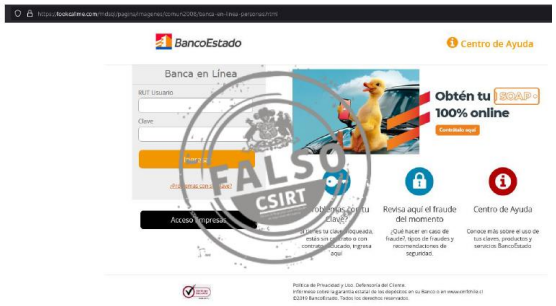
Imagen del mensaje

CSIRT alerta ante nuevo phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00600-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://valpa.digitalnoticias[.]com.mx/activacion/cuenta-tnbl/	
URL sitio falso	
https://bercante[.]xyz/1663956202/portada/personas/home.asp	
IP	
[149.57.153.151]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00600-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00600-01.pdf	

Imagen del }mensaje

CSIRT alerta de campaña de phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00601-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.skybrands.com[.]np/Recuperalo_Aqui/cuenta-sqft/	
URL sitio falso	
https://view.cavipando[.]xyz/1664198968/portada/personas/home.asp	
IP	
[68.65.122.77]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00601-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00601-01.pdf	

Imagen del sitio



CSIRT alerta de campaña de phishing suplantando SuperClave del Santander	
Alerta de seguridad cibernética	8FPH22-00602-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de septiembre de 2022
Última revisión	29 de septiembre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://nam10.safelinks[.]protection.outlook.com/?url=https%3A%2F%2Flinkprotect.cudasvc.com%2Furl%3Fa%3Dhttps%253a%252f%252fmaletashere.com%252fsantander.php%26c%3DE%2C1%2Cpi5x7VmivpdtdPj6sgtXDyflj3-i_pAExn7-PKWLOIiwelDpWR8tdgyOb5VRSC_DwABkLxrYRS0Fl2vguRA2V4xrgfZRxwdTr0R_YRu2H1sVKUcLxUzD8X4%2C%26typo%3D1&data=05%7C01%7Cwaleska.arteaga%40sea.gob.cl%7Cc91a54ca86644e8d006408daa001144f%7Cb71dc67ef57148469db81264f14ea88b%7C1%7C0%7C637998224384263779%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000%7C%7C%7C&sdata=ja%2B1nuxuz7i75ZajkMHjm1pSDvC2qQov0hT5K3ZdfYc%3D&reserved=0 https://maletashere[.]com/santander.php	
URL sitio falso	
https://bancosantander-	

cl.netsms[.]info/1664285301/portada/personas/home.asp
IP
[104.21.69.206]
Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/8fph22-00602-01/
https://www.csirt.gob.cl/media/2022/08/8FPH22-00602-01.pdf

Vulnerabilidades

CSIRT alerta de nuevas vulnerabilidades en Android	
Alerta de seguridad cibernética	9VSA22-00704-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022

CVE		
CVE-2022-22822	CVE-2021-0943	CVE-2022-22092
CVE-2022-23852	CVE-2022-26447	CVE-2022-22093
CVE-2022-23990	CVE-2021-0871	CVE-2022-22094
CVE-2022-25314	CVE-2022-20385	CVE-2022-25669
CVE-2022-20218	CVE-2022-20386	CVE-2022-25686
CVE-2022-20392	CVE-2022-20387	CVE-2022-25688
CVE-2022-20393	CVE-2022-20388	CVE-2022-25690
CVE-2022-20197	CVE-2022-20389	CVE-2022-25696
CVE-2022-20395	CVE-2022-20390	CVE-2022-20385
CVE-2022-20398	CVE-2022-20391	CVE-2022-20386
CVE-2022-20396	CVE-2022-25708	CVE-2022-20387
CVE-2022-20399	CVE-2022-22066	CVE-2022-20388
CVE-2021-4083	CVE-2022-22074	CVE-2022-20389
CVE-2022-29582	CVE-2022-22081	CVE-2022-20390
CVE-2021-0697	CVE-2022-22089	CVE-2022-20391
CVE-2021-0942	CVE-2022-22091	

Fabricantes
Android
Productos afectados
Dispositivos con sistema Android actualizado con anterioridad al parche 2022-09-01.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00704-01/
https://www.csirt.gob.cl/media/2022/09/9VSA22-00704-01.pdf

CSIRT alerta de nuevas vulnerabilidades en BIND 9	
Alerta de seguridad cibernética	9VSA22-00705-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de septiembre de 2022
Última revisión	23 de septiembre de 2022
CVE	
CVE-2022-2906 CVE-2022-3080 CVE-2022-38177 CVE-2022-38178	
Fabricantes	
BIND	
Productos afectados	
BIND 9.9.12 -> 9.9.13 9.10.7 -> 9.10.8 9.11.3 -> 9.16.32 9.18.0 -> 9.18.6 9.19.0 -> 9.19.4 BIND Supported Preview Edition 9.11.4-S1 -> 9.11.37-S1 9.16.8-S1 -> 9.16.32-S1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00705-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00705-01.pdf	

CSIRT informa de nueva vulnerabilidad crítica en Sophos Firewall	
Alerta de seguridad cibernética	9VSA22-00706-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	24 de septiembre de 2022
Última revisión	24 de septiembre de 2022
CVE	
CVE-2022-3236	
Fabricantes	
Sophos	
Productos afectados	
Sophos Firewall v19.0 MR1 (19.0.1) y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00706-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00706-01.pdf	
CSIRT alerta de vulnerabilidad en Zoho ManageEngine	

Alerta de seguridad cibernética	9VSA22-00707-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	26 de septiembre de 2022
Última revisión	26 de septiembre de 2022
CVE	
CVE-2022-35405	
Fabricantes	
Zoho	
Productos afectados	
Access Manager Plus versión 4302 y anteriores. Password Manager Pro versión 12100 y anteriores. PAM360 versión 5500 y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00707-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00707-01.pdf	

CSIRT alerta de vulnerabilidad en Pebble	
Alerta de seguridad cibernética	9VSA22-00708-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de septiembre de 2022
Última revisión	27 de septiembre de 2022
CVE	
CVE-2022-37767	
Fabricantes	
Pebble	
Productos afectados	
Pebble	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00708-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00708-01.pdf	

CSIRT comparte nuevas vulnerabilidades en WhatsApp y WhatsApp for Business	
Alerta de seguridad cibernética	9VSA22-00709-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de septiembre de 2022
Última revisión	27 de septiembre de 2022
CVE	
CVE-2022-36934 CVE-2022-27492	
Fabricantes	
Meta	
Productos afectados	
WhatsApp for Android anterior a 2.22.16.12 WhatsApp Business for Android anterior a 2.22.16.12 WhatsApp for iOS anterior a 2.22.16.12 WhatsApp Business for iOS anterior a 2.22.16.12 WhatsApp for Android anterior a v2.22.16.2, WhatsApp for iOS v2.22.15.9	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00709-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00709-01.pdf	

CSIRT comparte nueva vulnerabilidad en Microsoft Endpoint Configuration Manager	
Alerta de seguridad cibernética	9VSA22-00710-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	28 de septiembre de 2022
Última revisión	28 de septiembre de 2022
CVE	
CVE-2022-37972	
Fabricantes	
Microsoft	
Productos afectados	
Microsoft Endpoint Configuration Manager	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00710-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00710-01.pdf	

CSIRT alerta de vulnerabilidad en IBM WebSphere Application Server	
Alerta de seguridad cibernética	9VSA22-00711-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	28 de septiembre de 2022
Última revisión	28 de septiembre de 2022
CVE	
CVE-2022-35282	
Fabricantes	
IBM	
Productos afectados	
IBM WebSphere Application Server 7.0, 8.0, 8.5, y 9.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00711-01/	
https://www.csirt.gob.cl/media/2022/09/9VSA22-00711-01.pdf	

Actualidad

Alerta de Seguridad Cibernética: Ransomware en el Poder Judicial
Compartimos información sobre el ataque de ransomware sufrido por el Poder Judicial:
Detalles: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-ransomware-poder-judicial/

ACTUALIZACIÓN Alerta de Seguridad Cibernética: Ransomware en el Poder Judicial
Compartimos indicadores de compromiso y una descripción del comportamiento del ransomware LockBit Black, el que afectó al Poder Judicial. Detalles: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-nueva-vuln-sophos-firewall/

Alerta de Seguridad Cibernética: Nueva vulnerabilidad en Sophos Firewall (CVE-2022-3236)
Advertimos de una nueva campaña de explotación activa de una vulnerabilidad en Sophos Firewall. Detalles: csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-nueva-vuln-sophos-firewall/

Alerta de Seguridad Cibernética: Llamado a verificar actualizaciones y respaldos
Llamamos a las instituciones públicas del Estado, a las entidades en convenio de colaboración y a los administradores de sistemas y público en general a tomar las siguientes acciones, en vista de un incremento en los escaneos de reconocimiento observados por parte del CSIRT de Gobierno en la Red de Conectividad del Estado. Detalles: https://www.csirt.gob.cl/noticias/alerta-de-seguridad-cibernetica-actualizaciones-y-respaldos/

Ciberdiccionario Volumen 18

En el capítulo de esta semana de nuestro Ciberdiccionario compartimos más conceptos clave para el ejercicio de la ciberseguridad: incidente, indicadores de compromiso (IoC), vulnerabilidad y archivo ejecutable. También pueden ver y descargar estos consejos en PDF en nuestra web: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-17

Ciberconsejos | Cómo proteger nuestro correo institucional

Entregamos consejos para cuidar de nuestra ciberseguridad al usar una cuenta de email, especialmente cuando se trata de una casilla corporativa o institucional, las que suelen ser usadas por los ciberdelincuentes para acceder, a través de mensajes maliciosos (phishing) a las redes de una organización. También pueden ver estos consejos en nuestra web: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-correo-institucional/

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.

- Daniel Gutiérrez
- Jair Palma
- Lidia Edith Ríos Soto
- Gustavo Avaria Decombe
- Daily Mota