Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

14-10-2022 | Año 4 | N°171

Boletín de Seguridad Cibernética

Semana del 7 al 13 de octubre de 2022

La semana en cifras

Parches

112

para vulnerabilidades

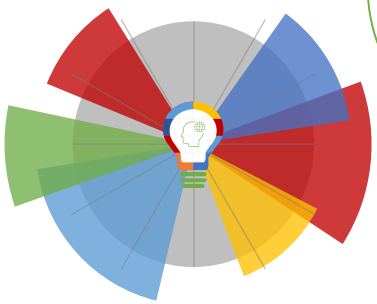
Las mitigaciones son útiles en productos de Fotinet, Microsoft, Zimbra, VMware, Palo Alto y Adobe.

IP

18

Informadas

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



Se advirtieron

31

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

3

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

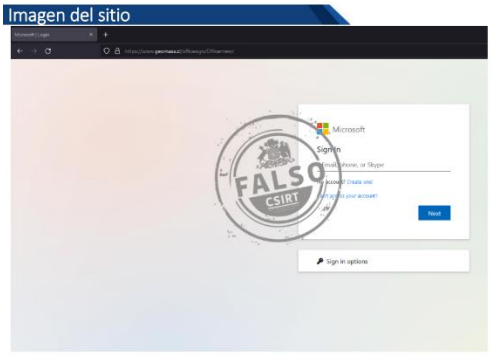
Malware

CSIRT alerta de campaña de phishing con malware disfrazado de factura	
Alerta de seguridad cibernética	2CMV22-00357-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
Indicadores de compromiso	
Asunto	
New Invoice(s) for C325170193 are Available to be Viewed	
Correo de salida	
emyczstz@glay.org	
SHA256	
685e7c77f49053fdbab826f1ff8a9349ae4173690d6bca6ae41676f1602fbb32	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00357-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00357-01.pdf	

CSIRT alerta de phishing con falso aviso de término de contrato	
Alerta de seguridad cibernética	2CMV22-00358-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022
Indicadores de compromiso	
Asunto	
RE: Aviso Término de Contrato	
Correo de Salida	
a.abdala.m@tie.cl	
SHA256	
pedido urgente pdf.exe.xz ac38b76d13701842fbf7a3ec0c549ea7008e4251b215b26d34c326daef0c0eae pedido urgente pdf.exe 58ba13b59f9427de31b01d4ac4b9bb6e9fd6f3ec7a53610c9d585884b768145e	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00358-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00358-01.pdf	

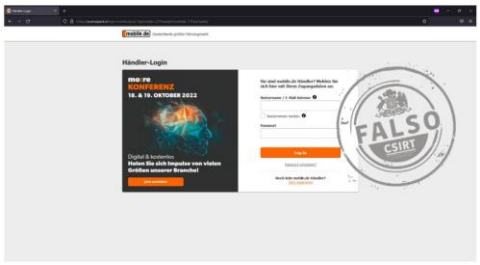
Sitios fraudulentos

Imagen del sitio



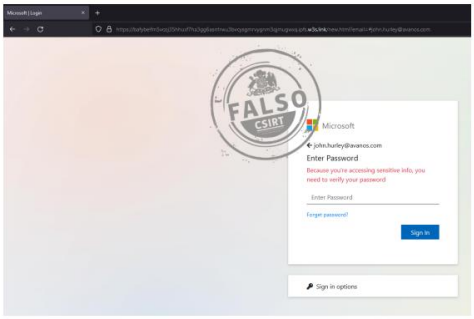
CSIRT alerta ante página fraudulenta que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR22-01112-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.geomass[.]cl/officesign/Officernew/	
IP	
[186.64.114.110]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01112-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01112-01.pdf	

Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta portal alemán de venta de autos	
Alerta de seguridad cibernética	8FFR22-01113-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://avanzapark.cl/login.mobile.de https://avanzapark.cl/login.mobile.de/a2-login/caller-22Fhandel/mobilede-11Fstartseite/	
IP	
[201.217.243.174]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01113-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01113-01.pdf	

Imagen del sitio

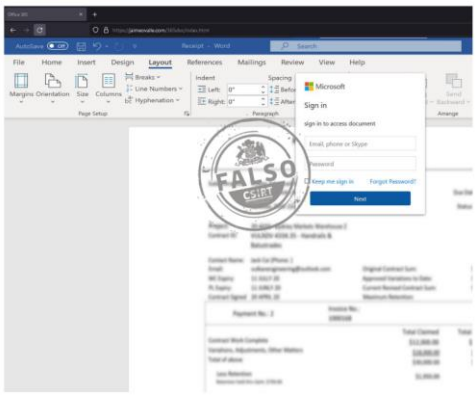


CSIRT alerta por sitio fraudulento que suplanta login de Microsoft	
Alerta de seguridad cibernética	8FFR22-01114-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
http://fidelis[.]cl/trillogy/yiuiriir/iniyt/9:55:59%20PM/john.hurley@avanos.com https://bafybeifm5vcoj35hhuxf7ha3gg6asrrlrwu3bvcysgmrvygnm3qjmugwxq.ipfs.w3s[.]link/new.html?email=#john.hurley@avanos.com	
IP	
[190.96.85.189]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01114-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01114-01-1.pdf	

Imagen del sitio

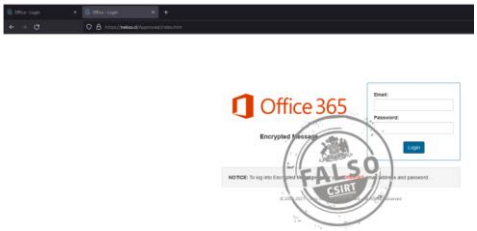
CSIRT alerta de página fraudulenta que suplanta a banco griego	
Alerta de seguridad cibernética	8FFR22-01115-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://steakit[.]cl/winb/Wino/default.php?id=163.247.70.80	
IP	
[192.185.188.94]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01115-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01115-01-1.pdf	

Imagen del sitio



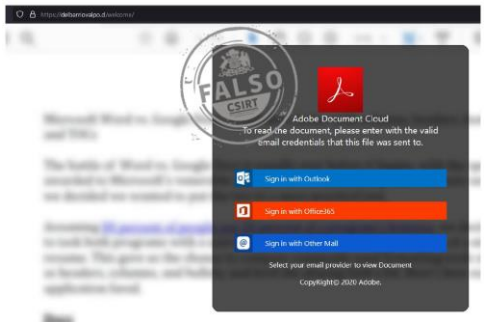
CSIRT alerta ante sitio fraudulento que suplanta a Microsoft	
Alerta de seguridad cibernética	8FFR22-01116-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://jaimeovalle[.]com/365doc/index.html	
IP	
[201.148.104.187]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01116-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01116-01.pdf	

Imagen del sitio



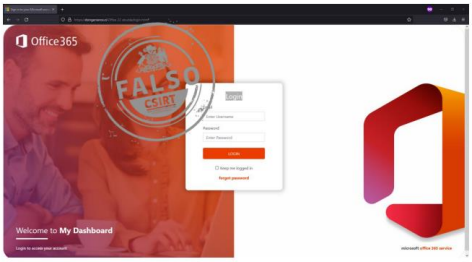
CSIRT alerta ante sitio fraudulento que suplanta a Office 365	
Alerta de seguridad cibernética	8FFR22-01117-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://nekxo[.]cl/Approved/ http://nekxo[.]cl/Approved/index.htm	
IP	
[200.63.97.54]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01117-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01117-01.pdf	

Imagen del sitio



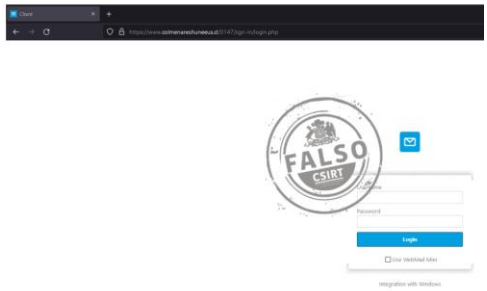
CSIRT alerta de página fraudulenta que suplanta al login de Adobe	
Alerta de seguridad cibernética	8FFR22-01118-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2022
Última revisión	12 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://delbarriovalpo[.]cl/welcome/	
IP	
[186.64.116.165]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01117-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01117-01.pdf	

Imagen del sitio



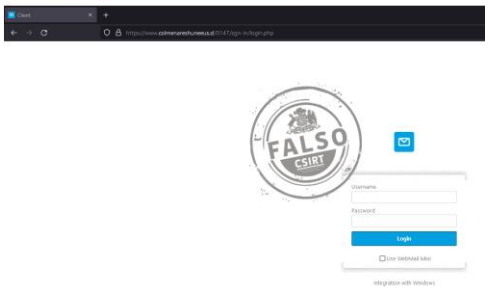
CSIRT alerta ante página fraudulenta que suplanta a Office 365	
Alerta de seguridad cibernética	8FFR22-01120-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2022
Última revisión	12 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
http://dsingenieros[.]cl/Office%2022%20double/login.html?xmv=iHu3GaWkcAETjPv&thpjkglgg=2P7kBGdOV5IqZNCR89cFLDBOd&dpb=UwwcrHUaAUMPzQ1Y&zqivkue=kYmUhn3oQBllHgtSj&vsfslvnk=CJk43jO1YDl5SIS3vJ32&goucweb=Se6kXQjIJtq3CsEgdz4OmBVwUO&yif=aiqhiZ4pMwhDqpr46oelH&jiqld=LFolfRPiMkusOyiD9NAs&pqdpgvsjk=sRZ1VFC3x2UEq3i6zk5IwL4J1qKUvG https://dsingenieros[.]cl/Office%2022%20double/login.html	
IP	
[186.64.119.160]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01120-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01120-01-1.pdf	

Imagen del sitio



CSIRT alerta de sitio fraudulento que suplanta a WebMail Mini	
Alerta de seguridad cibernética	8FFR22-01121-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2022
Última revisión	12 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
http://www.zenzero[.]cl/0147/rdt.html https://www.colmenareshuneeus[.]cl/0147/cgn-in/login.php	
IP	
[200.6.118.162]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01121-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01121-01.pdf	

Imagen del sitio



CSIRT alerta ante página fraudulenta que suplanta login de Webmail Mini	
Alerta de seguridad cibernética	8FFR22-01122-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2022
Última revisión	13 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://colegiosconcepcion[.]cl/zip/np/7rfhATh/test@csirt.gob.cl?aclid=3NNHYwAAAADxCQAAQanuO602-1iLXrg78QkAAPEJAAAAAAAAAVVNDQS1TYW4gRnJhbmNpc2NvAAAAAAAAAAAAAAAAAAAAAAAABAAAA https://bafybeicsapdb6iapble5huh6ph5gkjl75ugck7gnx4ih4w25zbx26hwfxy.ipfs.w3s[.]link/aws.html?email=test@csirt.gob.cl	
IP	
[104.18.22.52]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01122-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01122-01.pdf	

Imagen del sitio

CSIRT alerta de puerta fraudulenta que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01123-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2022
Última revisión	13 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://view.videocourse.me/1665693100/portada/personas/home.asp	
IP	
[160.153.248.232]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01123-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01123-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte nueva campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00611-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
Indicadores de compromiso	
URL redirección	
https://www.skybrands[.]com.np/Recuperalo_Aqui/cuenta-sqft/	
URL sitio falso	
https://manchetetom[.]click/1665157762/portada/personas/home.asp	
IP	
[47.87.146.254]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00611-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00611-01-1.pdf	

Imagen del mensaje

CSIRT alerta de campaña de phishing con falso email del Santander	
Alerta de seguridad cibernética	8FPH22-00612-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://nostracontrical[.]com/promociones/cuenta-ktoe/	
URL sitio falso	
https://privateban[.]click/1665166362/portada/personas/home.asp	
IP	
[47.87.146.12]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00612-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00612-01.pdf	

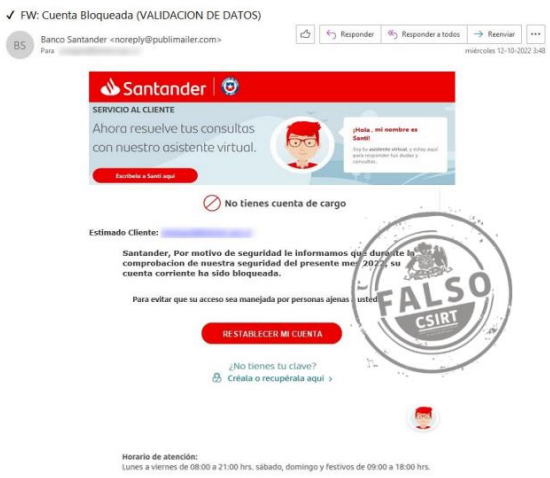
CSIRT alerta de campaña de phishing que suplanta al Santander

Alerta de seguridad cibernética	8FPH22-00613-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.skybrands[.]com.np/Recuperalo_Aqui/cuenta-ausd/	
URL sitio falso	
https://manchetetom[.]click/1665171689/portada/personas/home.asp	
IP	
[47.87.146.254]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00613-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00613-01.pdf	

Imagen del mensaje

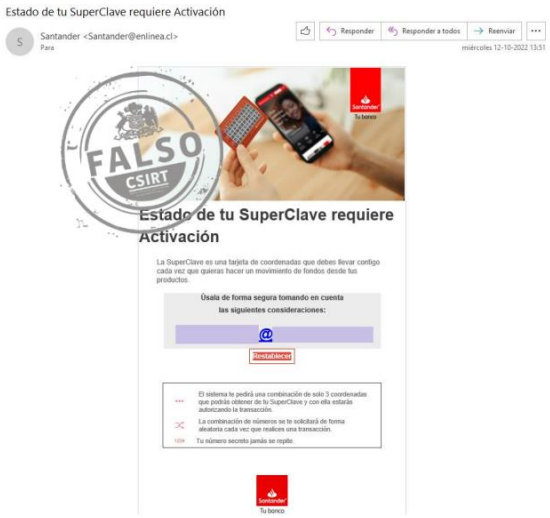
CSIRT alerta ante campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00614-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2022
Última revisión	12 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.skybrands.com[.]np/Recuperalo_Aqui/cuenta-ausd/	
URL sitio falso	
https://mduea.videocourse[.]me/1665502459/portada/personas/home.asp	
IP	
[160.153.248.232]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00614-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00614-01.pdf	

Imagen del mensaje



CSIRT alerta de sitio fraudulento que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00615-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2022
Última revisión	12 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.skybrands.com[.]np/Recuperalo_Aqui/cuenta-ausd/	
URL sitio falso	
http://surfinter[.]online/santanderpersonas/pagina/login.asp	
IP	
[72.167.56.2]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00615-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00615-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al Santander	
Alerta de seguridad cibernética	8FPH22-00616-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2022
Última revisión	12 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://superavance-cl[.]top/santander.php	
URL sitio falso	
https://brancosantander-cl.homes-cl[.]top/1665598433/portada/personas/home.asp	
IP	
[104.21.37.144]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00616-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00616-01.pdf	

Imagen del mensaje

CSIRT alerta ante campaña de phishing con falso aviso de emails

no recibidos	
Alerta de seguridad cibernética	8FPH22-00617-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de octubre de 2022
Última revisión	13 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://8035ugt-w34hrg-0hjwre-ghjew-r0hg-ehg9-h-rtg.obs.af-south-1.myhuaweicloud.com/y950tg-3-045hgt-0w3e4rhjg-0wejrg0-he5-0ghrtg.html?AWSAccessKeyId=Y33AQWKH1XTGWG0XAF5T&Expires=1666815540&Signature=G%2BnkJf3iAcnAvLaF0mAVhHGYee0%3D#test@interior.gov.cl	
URL sitio falso	
https://8035ugt-w34hrg-0hjwre-ghjew-r0hg-ehg9-h-rtg.obs.af-south-1.myhuaweicloud.com/y950tg-3-045hgt-0w3e4rhjg-0wejrg0-he5-0ghrtg.html?AWSAccessKeyId=Y33AQWKH1XTGWG0XAF5T&Expires=1666815540&Signature=G%2BnkJf3iAcnAvLaF0mAVhHGYee0%3D#test@interior.gov.cl	
IP	
[159.138.160.64]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00617-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00617-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidad crítica en firewall y proxies Fortinet	
Alerta de seguridad cibernética	9VSA22-00715-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
CVE	
CVE-2022-40684	
Fabricantes	
Fortinet	
Productos afectados	
FortiOS: 7.0.0 a 7.0.6 y de 7.2.0 a 7.2.1 FortiProxy: 7.0.0 a 7.0.6 y 7.2.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00715-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00715-01.pdf	

CSIRT alerta vulnerabilidad día cero en Zimbra Collaboration Suite	
Alerta de seguridad cibernética	9VSA22-00716-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de octubre de 2022
Última revisión	07 de octubre de 2022
CVE	
CVE-2022-41352	
Fabricantes	
Zimbra	
Productos afectados	
Zimbra Collaboration (ZCS) 8.8.15 and 9.0	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00716-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00716-01-1.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday Microsoft Octubre 2022	
Alerta de seguridad cibernética	9VSA22-00717-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de octubre de 2022
Última revisión	11 de octubre de 2022

CVE

CVE-2022-22035	CVE-2022-37993	CVE-2022-41043
CVE-2022-30198	CVE-2022-37991	CVE-2022-37968
CVE-2022-38043	CVE-2022-37990	CVE-2022-35829
CVE-2022-38041	CVE-2022-38038	CVE-2022-41032
CVE-2022-37986	CVE-2022-37989	CVE-2022-41042
CVE-2022-35770	CVE-2022-38037	CVE-2022-41081
CVE-2022-38040	CVE-2022-37988	CVE-2022-41038
CVE-2022-37987	CVE-2022-38033	CVE-2022-41037
CVE-2022-37997	CVE-2022-38032	CVE-2022-41036
CVE-2022-37994	CVE-2022-38031	CVE-2022-41034
CVE-2022-33635	CVE-2022-37982	CVE-2022-41033
CVE-2022-38045	CVE-2022-37977	CVE-2022-37981
CVE-2022-34689	CVE-2022-38029	CVE-2022-41031
CVE-2022-37965	CVE-2022-38034	CVE-2022-38001
CVE-2022-38046	CVE-2022-38036	CVE-2022-38003
CVE-2022-37976	CVE-2022-37978	CVE-2022-38053
CVE-2022-37995	CVE-2022-38025	CVE-2022-38051
CVE-2022-38021	CVE-2022-37974	CVE-2022-38050
CVE-2022-37984	CVE-2022-37973	CVE-2022-38049
CVE-2022-38028	CVE-2022-37998	CVE-2022-38000
CVE-2022-38022	CVE-2022-37980	CVE-2022-37996
CVE-2022-33634	CVE-2022-37970	CVE-2022-38048
CVE-2022-24504	CVE-2022-37983	CVE-2022-38027
CVE-2022-38026	CVE-2022-38016	CVE-2022-38044
CVE-2022-33645	CVE-2022-38030	CVE-2022-37999
CVE-2022-38042	CVE-2022-38039	CVE-2022-38047
CVE-2022-37985	CVE-2022-37979	CVE-2022-37971
CVE-2022-37975	CVE-2022-41083	CVE-2022-38017

Fabricantes

Microsoft

Productos afectados

Active Directory Domain Services
Azure
Azure Arc
Client Server Run-time Subsystem (CSRSS)
Microsoft Edge (Chromium-based)
Microsoft Graphics Component
Microsoft Office
Microsoft Office SharePoint

Microsoft Office Word
Microsoft WDAC OLE DB provider for SQL
NuGet Client
Remote Access Service Point-to-Point Tunneling Protocol
Role: Windows Hyper-V
Service Fabric
Visual Studio Code
Windows Active Directory Certificate Services
Windows ALPC
Windows CD-ROM Driver
Windows COM+ Event System Service
Windows Connected User Experiences and Telemetry
Windows CryptoAPI
Windows Defender
Windows DHCP Client
Windows Distributed File System (DFS)
Windows DWM Core Library
Windows Event Logging Service
Windows Group Policy
Windows Group Policy Preference Client
Windows Internet Key Exchange (IKE) Protocol
Windows Kernel
Windows Local Security Authority (LSA)
Windows Local Security Authority Subsystem Service (LSASS)
Windows Local Session Manager (LSM)
Windows NTFS
Windows NTLM
Windows ODBC Driver
Windows Perception Simulation Service
Windows Point-to-Point Tunneling Protocol
Windows Portable Device Enumerator Service
Windows Print Spooler Components
Windows Resilient File System (ReFS)
Windows Secure Channel
Windows Security Support Provider Interface
Windows Server Remotely Accessible Registry Keys
Windows Server Service
Windows Storage
Windows TCP/IP
Windows USB Serial Driver
Windows Web Account Manager
Windows Win32K
Windows WLAN Service
Windows Workstation Service
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00717-01/
https://www.csirt.gob.cl/media/2022/10/9VSA22-00717-01.pdf

CSIRT alerta de vulnerabilidades en varios productos de Adobe		
Alerta de seguridad cibernética	9VSA22-00718-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	12 de octubre 2022	
Última revisión	12 de octubre 2022	
CVE		
CVE-2022-35712	CVE-2022-38421	CVE-2022-38444
CVE-2022-35690	CVE-2022-38422	CVE-2022-38445
CVE-2022-35711	CVE-2022-42340	CVE-2022-38446
CVE-2022-38418	CVE-2022-38424	CVE-2022-38447
CVE-2022-35710	CVE-2022-42341	CVE-2022-38448
CVE-2022-38423	CVE-2022-38440	CVE-2022-38450
CVE-2022-38419	CVE-2022-38441	CVE-2022-42339
CVE-2022-38420	CVE-2022-38442	
Fabricantes		
Adobe		
Productos afectados		
ColdFusion 2018 14 y anteriores, 2021 4 y anteriores. Dimension 3.4.5 y anteriores. Acrobat DC 22.002.20212 y anteriores. Acrobat Reader DC 22.002.20212 y ant., 2020 20.005.30381 y ant. Acrobat 2020 20.005.30381 y anteriores Commerce 2.4.4-p1 y anteriores, 2.4.5 y anteriores. Magento Open Source 2.4.4-p1 y anteriores, 2.4.5 y anteriores		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00718-01/		
https://www.csirt.gob.cl/media/2022/10/9VSA22-00718-01.pdf		

CSIRT alerta de vulnerabilidad en PAN-OS 8.1	
Alerta de seguridad cibernética	9VSA22-00719-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	12 de octubre 2022
Última revisión	12 de octubre 2022
CVE	
CVE-2022-0030	
Fabricantes	
Palo Alto	
Productos afectados	
PAN-OS 8.1 anteriores a 8.1.24.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00719-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00719-01.pdf	

CSIRT alerta vulnerabilidades en productos VMware	
Alerta de seguridad cibernética	9VSA22-00720-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	12 de octubre 2022
Última revisión	12 de octubre 2022
CVE	
CVE-2022-31680 CVE-2022-31681 CVE-2022-31682	
Fabricantes	
VMware	
Productos afectados	
VMware ESXi VMware vCenter Server (vCenter Server) VMware Cloud Foundation (Cloud Foundation)	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00720-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00720-01.pdf	

Actualidad

10CND22-00084-05 Alerta de Seguridad Cibernética | Vulnerabilidades día cero en Microsoft

Compartimos la más reciente actualización de las recomendaciones que entrega Microsoft sobre dos vulnerabilidades de día cero que afectan a los servidores Exchange en sus versiones 2013, 2016 y 2019, las cuales aún no cuentan con un parche definitivo.

Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00084-05/

Ciberconsejos en el Mes de la Ciberseguridad

Con motivo del Mes de la Ciberseguridad, continuamos con una segunda semana con importantes consejos para mejorar nuestra seguridad informática, los que pueden ser vistos aquí: https://www.csirt.gob.cl/recomendaciones/mes-de-la-ciberseguridad/.

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.

- Javier Lara Vivar
- Bárbara Palacios Cabezas
- Bastián Cristián González Acevedo
- Gustavo
- Pablo Araya del Pino
- Yanina Quilacán Fuentes
- Iván Leiva
- Kevin Anguita
- Adolfo Figueroa