Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

28-10-2022 | Año 4 | N°173

Boletín de Seguridad Cibernética

Semana del 21 al 27 de octubre de 2022

La semana en cifras

Parches

156

para vulnerabilidades

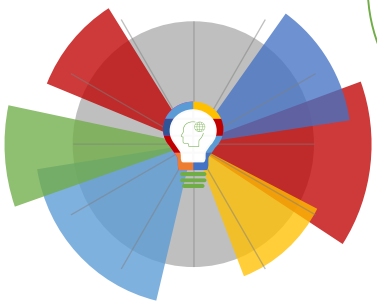
Las mitigaciones son útiles en productos de Apple, VMware, Atlassian, F5 y Linux.

IP

8

Informadas

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



Se advirtieron

16

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

34

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 ante phishing que suplanta a la Tesorería	
Alerta de seguridad cibernética	2CMV22-00362-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2022
Última revisión	21 de octubre de 2022

Indicadores de compromiso

Asunto

Informacion TGR de factura electronica
Notificacion TGR

Correo de Salida

root@contactoclsii1.infomenoemail.com
root@contactoclsii10.infomenoemail.com
root@contactoclsii11.infomenoemail.com
root@contactoclsii12.infomenoemail.com
root@contactoclsii13.infomenoemail.com
root@contactoclsii14.infomenoemail.com
root@contactoclsii15.infomenoemail.com
root@contactoclsii16.infomenoemail.com
root@contactoclsii2.infomenoemail.com
root@contactoclsii3.infomenoemail.com
root@contactoclsii4.infomenoemail.com
root@contactoclsii5.infomenoemail.com
root@contactoclsii6.infomenoemail.com
root@contactoclsii7.infomenoemail.com
root@contactoclsii8.infomenoemail.com
root@contactoclsii9.infomenoemail.com

SHA256

Nombre: 00F1S56789S0W1PAGO198CCS716.zip
SHA256:
4fd239fb48b377bf8ea5165548643bbf0bcc24183e0de92bd39bd0f85da53f8c
Nombre: 00F1S56789S0W1PAGO198CCS716.msi
SHA256:
ca4519fc650d94793df6cc7045548946c49dcfde58891d8afd1c38103a297d12
Nombre: MSICA59.tmp
SHA256:
44ffc4959be0ddb18b02d59c75e78e3e721992e362a2f90cae19adb3271886b9
MSID0A8.tmp
SHA256:
02db56648dcefdbe8ed8801f52372370982b3be5660007012f96884db5c4eef7

Enlaces para revisar el informe:
https://www.csirt.gob.cl/alertas/2cmv22-00362-01/
https://www.csirt.gob.cl/media/2022/10/2CMV22-00362-01.pdf

CSIRT alerta ante campaña de phishing con falso documento comercial	
Alerta de seguridad cibernética	2CMV22-00363-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2022
Última revisión	21 de octubre de 2022
Indicadores de compromiso	
Asunto	
S31030 – CTJV- Offer Request	
Correo de Salida	
info@webcp.live	
SHA256	
Nombre: Offer_CTJV.gz SHA256: a284fe0ba3ca99fb776ffcff4ca1da7a839bcbd301e4b07aea056ef5ce3909d3 Nombre: Offer_CTJV.exe SHA256: 3c6e68b6ac37e83297be2aa9555684046a464cfaceb90ed6a575c7d31ec0cffa Nombre: UUt.exe SHA256: c0724d08b48f7e225be261806063b1364ce6a310cbfd37d6a3dba47e7f4021e4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00363-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00363-01.pdf	

CSIRT alerta de phishing con falso váucher de pago	
Alerta de seguridad cibernética	2CMV22-00364-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2022
Última revisión	21 de octubre de 2022
Indicadores de compromiso	
Asunto	
[NOTIFICACIÓN] Váucher de pago de liquidación	
Correo de Salida	
ventas5@acerosryasa.com	
SHA256	
Nombre: COMPROBANTE-PAGO.zip SHA256: 850bc62292e8907fd10987dba6f41b1fe6b9703db32a795bf3005c8697d45605 Nombre: COMPROBANTE-PAGO.html SHA256: 3ec1a6767c73a79d09064753c8e6cbf1304cd9470882ef011018c17025f1735d Nombre: COMPROBANTE-ELECTRONICO-PAGO-Estado Liquidado-SPEI-.zip SHA256: 60e435a89644ce48ea75fb2cb78143922df7d4ab4f6916b17da64220a640f875 Nombre: CEP_COMPROBANTE-ELECTRONICO-PAGO-CEP-41136d968a589ee7f4bf39cd15d31bd8e9fc.msi SHA256: 2dbf089f402f3a36ec994071700110700f68f581838aa1c61eef7ea5672d4f79 Nombre: MSI2952.tmp SHA256: 44ffc4959be0ddb18b02d59c75e78e3e721992e362a2f90cae19adb3271886b9 Nombre: MSI3CC0.tmp SHA256: 9cef2f9a93dffcbb38273ec09eb96216010ecc6e9d7129bb62806d933605084d	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00364-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00364-01.pdf	

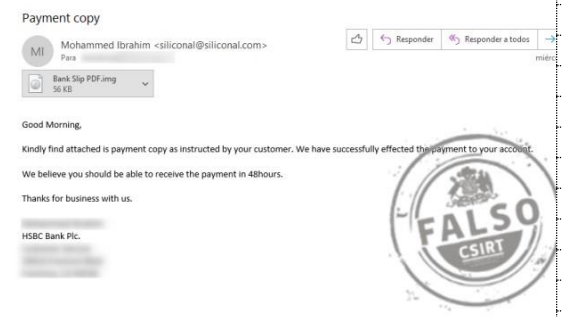
CSIRT alerta ante campaña de phishing con malware que suplanta a la TGR	
Alerta de seguridad cibernética	2CMV22-00365-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2022
Última revisión	24 de octubre de 2022
Indicadores de compromiso	
Asunto	
Informacion ☆ TGR de factura electronica	
Correo de Salida	
viv@viv.az	
SHA256	
Nombre: 00C4T331L024S67DE821II.zip SHA256: 4fd239fb48b377bf8ea5165548643bbf0bcc24183e0de92bd39bd0f85da53f8c Nombre: 00C4T331L024S67DE821II.msi SHA256: ca4519fc650d94793df6cc7045548946c49dcfde58891d8afd1c38103a297d12 Nombre: MSI700F.tmp SHA256: 44ffc4959be0ddb18b02d59c75e78e3e721992e362a2f90cae19adb3271886b9 Nombre: MSIFBDA.tmp SHA256: 67b0763fa0c849e0fa4e9159f48cc8adf9684dd62a55a6379d5ff1a4215af87f	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00365-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00365-01.pdf	

CSIRT alerta ante phishing con malware que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV22-00366-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2022
Última revisión	24 de octubre de 2022
Indicadores de compromiso	
Asunto	
FW: Informacion TGR de factura electronica	
Correo de Salida	
root@contactoclsii16.infomenoemail.com	
SHA256	
Nombre: 0G88S020UD450D04D.zip SHA256: 68ace1238716909d94253277e839c10827c262fc06898a6fce58a67a0648dcc9 Nombre: 0G88S020UD450D049H1.msi SHA256: 8a4cd222ccba2454b70f66c7827df4801af011a33cb1de6493287e5a1e298fe1 Nombre: MSI77B5.tmp SHA256: 44ffc4959be0ddb18b02d59c75e78e3e721992e362a2f90cae19adb3271886b9 Nombre: MSI7DC5.tmp SHA256: d2aa671e879005b898e0706e576131e6c24104f52e667234aa7ae8fea511260a	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00366-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00366-01.pdf	

CSIRT alerta de campaña de phishing que suplanta a la TGR	
Alerta de seguridad cibernética	2CMV22-00367-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2022
Última revisión	27 de octubre de 2022
Indicadores de compromiso	
Asunto	
FW: Informacion TGR de factura electronica FW: Notificacion TGR	
Correo de Salida	
root@contactoclsii16.infomenoemail.com root@contactoclsii2.infomenoemail.com root@contactoclsii11.infomenoemail.com root@contactoclsii15.infomenoemail.com root@contactoclsii14.infomenoemail.com root@contactoclsii6.infomenoemail.com root@contactoclsii5.infomenoemail.com root@contactoclsii8.infomenoemail.com root@contactoclsii1.infomenoemail.com root@contactoclsii12.infomenoemail.com root@contactoclsii7.infomenoemail.com root@contactoclsii9.infomenoemail.com root@contactoclsii4.infomenoemail.com	
SHA256	
Nombre: 00F1S56789S0W1PAGO198CCS716.zip SHA256: 4fd239fb48b377bf8ea5165548643bbf0bcc24183e0de92bd39bd0f85da53f8c Nombe: 00F1S56789S0W1PAGO198CCS716.msi SHA256: ca4519fc650d94793df6cc7045548946c49dcfde58891d8afd1c38103a297d12 Nombre: MSICA59.tmp SHA256: 44ffc4959be0ddb18b02d59c75e78e3e721992e362a2f90cae19adb3271886b9 Nombre: MSID0A8.tmp SHA256: 02db56648dcefdbe8ed8801f52372370982b3be5660007012f96884db5c4eef7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00367-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00367-01.pdf	

CSIRT alerta de phishing que suplanta a DHL	
Alerta de seguridad cibernética	2CMV22-00368-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2022
Última revisión	27 de octubre de 2022
Indicadores de compromiso	
Asunto	
DHL Pending delivery	
Correo de Salida	
donsh@fhhl.com	
SHA256	
Nombre: DHL_924820.IMG SHA256: bf260ff15e0a10357980937576f516a75d209be93fdfe6852dc0f8cb5be34024 Nombre: JWBHBWZC.EXE SHA256 2193931688547621ee5c9ec01922784fb7d3ee91ff65f5f59db006b97c5a0d7a Nombre: zrD8ZJWA.json SHA256: b45d1dda071c8ee6b1078e8f71661ee1511887daf491a9f81415232a3c3bd631 Nombre: License.XenArmor SHA256: 212173a405c78d70f90e8ec0699a60ed2f4a9f3a8070de62eabd666c268fb174 Nombre: Unknown.dll SHA256: 568da887725ccfdc4c5aae3ff66792fe60eca4e0818338f6a8434be66a6fe46d Nombre: unk.xml SHA256: b45d1dda071c8ee6b1078e8f71661ee1511887daf491a9f81415232a3c3bd631 Nombre: zrD8ZJWA.exe SHA256: 63a7295e66183379580db16d0d191bb261ccc9edb982980051291c8bdf6c4ade	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00368-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00368-01.pdf	

Imagen del Mensaje



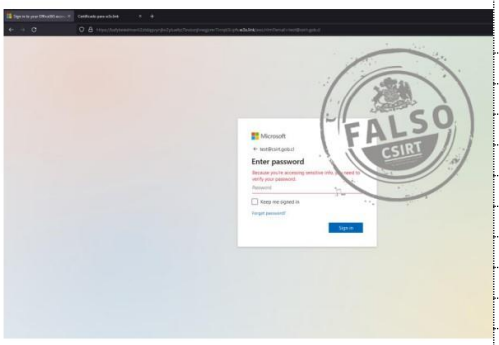
CSIRT alerta ante campaña de phishing con malware, que suplanta al HSBC	
Alerta de seguridad cibernética	2CMV22-00369-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2022
Última revisión	27 de octubre de 2022
Indicadores de compromiso	
Asunto	
Payment copy	
Correo de Salida	
siliconal@siliconal.com	
SHA256	
Nombre: Bank Slip PDF.img SHA256: d9d9b173feb5156303bc08de2856a6ee0a2ad7316cac0a032cea3eb638ce6de2 Nombre: 555666777.exe SHA256: d9d9b173feb5156303bc08de2856a6ee0a2ad7316cac0a032cea3eb638ce6de2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00369-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00369-01.pdf	

Sitios fraudulentos

Imagen del sitio

CSIRT alerta de sitio falso que suplanta a Netflix	
Alerta de seguridad cibernética	8FFR22-01128-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2022
Última revisión	24 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://www.netflixupdate.istylestore[.]cl/redirect/	
https://www.netflixupdate.istylestore[.]cl/redirect/N/login	
IP	
[186.64.114.25]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01128-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01128-01.pdf	

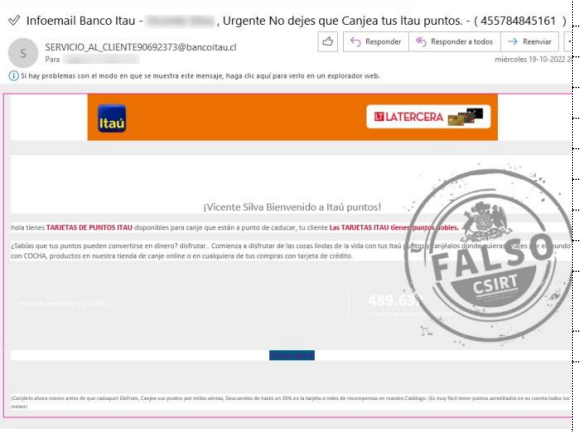
Imagen del sitio



CSIRT alerta ante sitio fraudulento que suplanta el login de Microsoft	
Alerta de seguridad cibernética	8FFR22-01129-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de octubre de 2022
Última revisión	25 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
http://colegiosconcepcion[.]cl/zip/np/10/15/2022/test@csirt.gob.cl	
https://bafybeiedmavti2ztdqgvynjbv2ytuefcz7bvzxzxjlvwgjzrer7inrqk5i.ipfs.w3s[.]link/awz.html?email=test@csirt.gob.cl	
IP	
[200.35.157.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01129-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01129-01.pdf	

Phishing

Imagen del mensaje

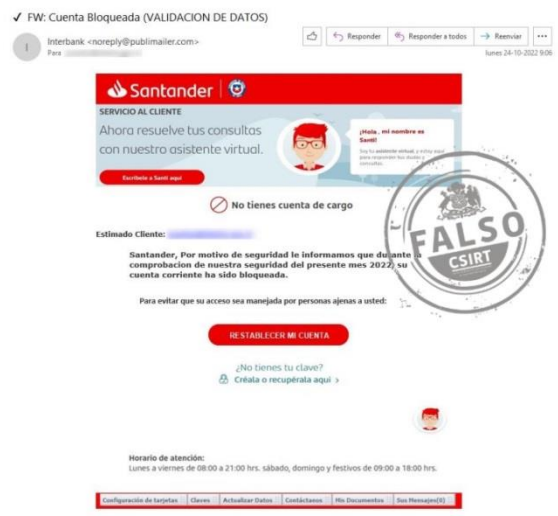


CSIRT alerta ante phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00624-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2022
Última revisión	21 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.igramarmorrojable.com/wp-content/languages/–/https:/bancoitau.cl/?cliente=test@csirt.gob.cl	
URL sitio falso	
https://rescatetuspuntosahora.com/App34b21c3/access.php?verify=D1CXJBRBD1CX-XXRP-D1CXXXRPXXRP-MHRVXXRP&sessionUser=d4kqadhofomlbhcalag0ie25gt&userLogin=45c48cce2e2d7fbdea1afc51c7c6ad26&queryString=	
IP	
[20.226.60.161]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00624-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00624-01.pdf	

Imagen} del mensaje

CSIRT alerta de phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00625-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de octubre de 2022
Última revisión	21 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://www.igramarmorrojable.com/wp-content/languages/–/https:/empresas.bancoitau.cl/?cliente=test@csirt.gob.cl	
URL sitio falso	
https://rescatetuspuntosahora.com/App6102863/access.php?verify=DPY39CMUDPY3-8ALT-DPY38ALT8ALT-9Q1P8ALT&sessionUser=d4kqadhofomlbhcalag0ie25gt&userLogin=c74d97b01eae257e44aa9d5bade97baf&queryString=	
IP	
[161.97.74.126]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00625-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00625-01.pdf	

Imagen del mensaje



CSIRT alerta por nueva campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00626-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2022
Última revisión	24 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://surfsantnder.info/activacion/cuenta-kand/	
URL sitio falso	
https://broncopatito.xyz/1666614320/portada/personas/home.asp	
IP	
[199.33.112.226]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00626-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00626-01.pdf	

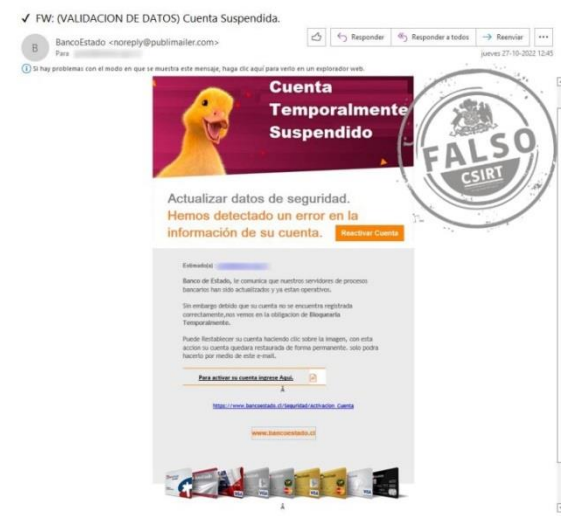
Imagen del mensaje

CSIRT alerta de nueva campaña de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH22-00627-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2022
Última revisión	24 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://wedsrtl.000webhostapp.com/ronda.com.html	
URL sitio falso	
https://wedsrtl.000webhostapp.com/ronda.com.html	
IP	
[145.14.145.88]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00627-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00627-01.pdf	

Imagen del mensaje

CSIRT alerta de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH22-00629-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de octubre de 2022
Última revisión	25 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://heyflow.id/correo#start	
URL sitio falso	
https://heyflow.id/correo#start	
IP	
[216.239.32.21]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00629-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00629-01.pdf	

Imagen del mensaje



CSIRT alerta de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00630-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2022
Última revisión	27 de octubre de 2022
Indicadores de compromiso	
URL redirección	
https://www.skybrands[.]com.np/Recuperalo_Aqui/cuenta-dgao/	
URL sitio falso	
https://broncopatito[.]site/1666898530/imagenes/_personas/home/default.asp	
IP	
[47.87.230.18]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00630-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00630-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades en productos de F5		
Alerta de seguridad cibernética	9VSA22-00731-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	21 de octubre de 2022	
Última revisión	21 de octubre de 2022	
CVE		
CVE-2022-36795	CVE-2022-41742	CVE-2022-41813
CVE-2022-41617	CVE-2022-41743	CVE-2022-41832
CVE-2022-41624	CVE-2022-41770	CVE-2022-41833
CVE-2022-41691	CVE-2022-41780	CVE-2022-41835
CVE-2022-41694	CVE-2022-41787	CVE-2022-41836
CVE-2022-41741	CVE-2022-41806	CVE-2022-41983
Fabricante		
F5		
Productos afectados		
BIG-IP (Advanced WAF, ASM) 14.1.5		
BIG-IP (Advanced WAF, ASM) 16.1.0 – 16.1.2		
BIG-IP (Advanced WAF, ASM) 16.1.0 – 16.1.3		
BIG-IP (Advanced WAF, ASM) 17.0.0		
BIG-IP (AFM) 16.1.0 – 16.1.3		
BIG-IP (AFM, PEM) 16.1.0 – 16.1.3		
BIG-IP (todos los módulos) 13.1.0 – 13.1.5		
BIG-IP (todos los módulos) 16.1.0 – 16.1.2		
BIG-IP (todos los módulos) 16.1.0 – 16.1.3		
BIG-IP (todos los módulos) 17.0.0		
BIG-IP (DNS, LTM con licencia DNS Services) 17.0.0		
BIG-IQ Centralized Management 8.0.0 – 8.2.0		
F5OS-A 1.0.0 – 1.0.1		
F5OS-C 1.1.0 – 1.3.2		
F5OS-C 1.3.0 – 1.3.2		
NGINX App Protect WAF 3.0.0 – 3.11.0		
NGINX Ingress Controller 2.0.0 – 2.4.0		
NGINX Open Source 1.23.0 – 1.23.1		
NGINX Plus R22 – R27		
R1 P1		
R2 P1		
R26 P1		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00731-01/		
https://www.csirt.gob.cl/media/2022/10/9VSA22-00731-01.pdf		

CSIRT alerta ante vulnerabilidad crítica en el kernel de Linux	
Alerta de seguridad cibernética	9VSA22-00732-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de octubre de 2022
Última revisión	24 de octubre de 2022
CVE	
CVE-2021-3493	
Fabricante	
Linux	
Productos afectados	
Linux Kernel	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00732-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00732-01.pdf	

CSIRT comparte vulnerabilidades resueltas por macOS Ventura 13		
Alerta de seguridad cibernética	9VSA22-00733-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	25 de octubre de 2022	
Última revisión	25 de octubre de 2022	
CVE		
CVE-2021-36690	CVE-2022-2000	CVE-2022-32913
CVE-2021-39537	CVE-2022-2042	CVE-2022-32914
CVE-2022-0261	CVE-2022-2124	CVE-2022-32915
CVE-2022-0318	CVE-2022-2125	CVE-2022-32918
CVE-2022-0319	CVE-2022-2126	CVE-2022-32922
CVE-2022-0351	CVE-2022-26730	CVE-2022-32924
CVE-2022-0359	CVE-2022-28739	CVE-2022-32928
CVE-2022-0361	CVE-2022-29458	CVE-2022-32934
CVE-2022-0368	CVE-2022-32205	CVE-2022-32936
CVE-2022-0392	CVE-2022-32206	CVE-2022-32938
CVE-2022-0554	CVE-2022-32207	CVE-2022-32940
CVE-2022-0572	CVE-2022-32208	CVE-2022-32947
CVE-2022-0629	CVE-2022-32827	CVE-2022-42788
CVE-2022-0685	CVE-2022-32858	CVE-2022-42789
CVE-2022-0696	CVE-2022-32862	CVE-2022-42790
CVE-2022-0714	CVE-2022-32864	CVE-2022-42791
CVE-2022-0729	CVE-2022-32865	CVE-2022-42793
CVE-2022-0943	CVE-2022-32866	CVE-2022-42795
CVE-2022-1381	CVE-2022-32867	CVE-2022-42796
CVE-2022-1420	CVE-2022-32870	CVE-2022-42799
CVE-2022-1616	CVE-2022-32875	CVE-2022-42806

CVE-2022-1619	CVE-2022-32879	CVE-2022-42808
CVE-2022-1620	CVE-2022-32881	CVE-2022-42809
CVE-2022-1621	CVE-2022-32883	CVE-2022-42811
CVE-2022-1622	CVE-2022-32886	CVE-2022-42813
CVE-2022-1629	CVE-2022-32888	CVE-2022-42814
CVE-2022-1674	CVE-2022-32890	CVE-2022-42815
CVE-2022-1720	CVE-2022-32892	CVE-2022-42818
CVE-2022-1725	CVE-2022-32895	CVE-2022-42819
CVE-2022-1733	CVE-2022-32898	CVE-2022-42820
CVE-2022-1735	CVE-2022-32899	CVE-2022-42823
CVE-2022-1769	CVE-2022-32902	CVE-2022-42824
CVE-2022-1851	CVE-2022-32904	CVE-2022-42825
CVE-2022-1897	CVE-2022-32905	CVE-2022-42829
CVE-2022-1898	CVE-2022-32908	CVE-2022-42830
CVE-2022-1927	CVE-2022-32911	CVE-2022-42831
CVE-2022-1942	CVE-2022-32912	CVE-2022-42832
CVE-2022-1968		
Fabricantes		
Apple		
Productos afectados		
MacOS		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00733-01/		
https://www.csirt.gob.cl/media/2022/10/9VSA22-00733-01.pdf		

CSIRT alerta ante vulnerabilidades en Atlassian Jira Align	
Alerta de seguridad cibernética	9VSA22-00734-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	25 de octubre de 2022
Última revisión	25 de octubre de 2022
CVE	
CVE-2022-36802 CVE-2022-36803	
Fabricantes	
Atlassian	
Productos afectados	
Atlassian Jira Align 10.107.4	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00734-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00734-01.pdf	

CSIRT comparte vulnerabilidades parchadas en iOS 16.1 y en iPadOS 16		
Alerta de seguridad cibernética	9VSA22-00735-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	26 de octubre de 2022	
Última revisión	26 de octubre de 2022	
CVE		
CVE-2022-42827	CVE-2022-42806	CVE-2022-42832
CVE-2022-42825	CVE-2022-32924	CVE-2022-42811
CVE-2022-32940	CVE-2022-42808	CVE-2022-32938
CVE-2022-42813	CVE-2022-42827	CVE-2022-42799
CVE-2022-32946	CVE-2022-42829	CVE-2022-42823
CVE-2022-32947	CVE-2022-42830	CVE-2022-42824
CVE-2022-42820	CVE-2022-42831	CVE-2022-32922
Fabricantes		
Apple		
Productos afectados		
IPhone 8 y posteriores, todos los modelos de iPad Pro, iPad Air tercera generación y posteriores, iPad de quinta generación y posteriores, iPad mini quinta generación y posteriores.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00735-01/		
https://www.csirt.gob.cl/media/2022/10/9VSA22-00735-01.pdf		

CSIRT alerta de vulnerabilidades en VMware	
Alerta de seguridad cibernética	9VSA22-00736-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	27 de octubre de 2022
Última revisión	27 de octubre de 2022
CVE	
CVE-2021-39144 CVE-2022-31678	
Fabricantes	
VMware	
Productos afectados	
VMware Cloud Foundation y VMware Cloud Foundation (NSX-V).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00736-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00736-01.pdf	

Actualidad

Alerta de Seguridad Cibernética | Fin de vida Red Hat JBoss Enterprise Application Platform 5.X

Desde el Equipo de Repuesta a Incidentes de Seguridad Informática del Ministerio del Interior, CSIRT de Gobierno, llamamos a los actores del ciberespacio nacional que ocupen Red Hat JBoss Enterprise Application Platform a verificar que se encuentre debidamente actualizado (al menos a las versiones 6.x), teniendo en consideración que las versiones 5.x ELS 2 tiene definido su fin de vida para el 30 de noviembre del presente año, y las versiones anteriores ya no cuentan con soporte alguno ni actualizaciones de seguridad.

Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00085-01/

Ley Marco sobre Ciberseguridad es aprobada en general por el Senado

Este 18 de octubre, el Senado aprobó, en general y por unanimidad de los presentes, el proyecto de Ley Marco sobre Ciberseguridad e Infraestructura Crítica, que entre sus disposiciones crea la Agencia Nacional de Ciberseguridad.

Ahora tocará su discusión en particular por parte de las comisiones de Defensa y Seguridad Pública del Senado, unidas, cuyos miembros presentarán sus indicaciones al proyecto hasta el 11 de noviembre, antes de continuar su tramitación.

Una de las principales medidas que define la iniciativa, en su versión actual, es la creación de la Agencia Nacional de Ciberseguridad (ANC), la cual tiene como fin asesorar al Presidente en la protección del ciberespacio nacional y coordinar las distintas instituciones a cargo de la ciberseguridad del país.

Detalles: https://www.csirt.gob.cl/noticias/ley-marco-senado/

Ciberguía | Malware y sus consecuencias

El malware es un programa o código malicioso diseñado intencionalmente para causar daño a cualquier clase de dispositivos como computadoras, teléfonos móviles, dispositivos IoT y a toda una infraestructura de red. Al ejecutar (abrir) un malware, las consecuencias podrían ser múltiples: anuncios molestos, robo de datos personales o sensibles, pérdida del control del equipo, envío de correos sin consentimiento, encriptar archivos y otras amenazas dependiendo el tipo de infección.

Existen distintos tipos, con características y forma de propagarse diferentes. ¿Cómo prevenir y qué hacer en caso de infectarse con un malware? Encuentra esta información y más en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/malware-y-sus-consecuencias/

Ciberdiccionario Volumen 21

El CSIRT de Gobierno compartió un nuevo volumen del ciberdiccionario. Esta semana explicamos qué es: código malicioso, rootkit, keylogger y dropper. Pueden ver estas definiciones también aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-21/.

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.

- Camila Cruz Rojas
- Juan Carlos Rodríguez López
- Christian Abarca
- Javier Lara Vivar
- Bárbara Alejandra García Rojas