Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

04-02-2022 | Año 4 | N°135

Boletín de Seguridad Cibernética

Semana del 28 de enero al 03 de febrero de 2022

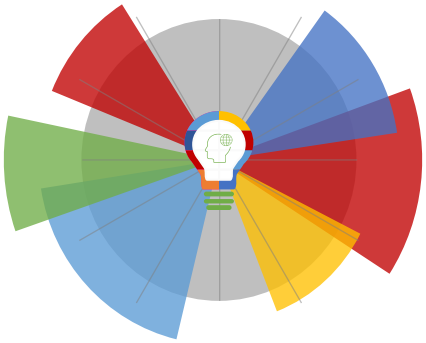
La semana en cifras

Hash

3

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

5

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

32

para vulnerabilidades

Las mitigaciones son útiles en productos Apache, Apple, Samba y Google.

IP

4

Informadas

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

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

Contenido

Sitios fraudulentos

CSIRT advierte sitio web que suplanta al Banco Estado	
Alerta de seguridad cibernética	8FFR22-01051-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2022
Última revisión	28 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://pustaka-smpn3tpi[.]com/smschile/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[202.74.236.112]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01051-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01051-01.pdf	

CSIRT informa falso sitio web del Banco Falabella	
Alerta de seguridad cibernética	8FFR22-01052-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2022
Última revisión	28 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
hXXp://www-falabella-cl.entrepreneurshipfoundationinc[.]org/login	
IP	
[158.106.130.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01052-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01052-01.pdf	

Phishing

CSIRT alerta sobre phishing con supuestos problemas en la cuenta de PayPal	
Alerta de seguridad cibernética	8FPH22-00468-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2022
Última revisión	28 de enero de 2022
Indicadores de compromiso	
URL redirección	
hXXps://mailtrack[.]io/trace/link/96796a1fc8f59d75bc5ba55f247adcb4a783579d	
URL sitio falso	
hXXps://berquo.insurt.bilekasnika[.]com/sign	
IP	
[164.90.196.193]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00468-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00469-01.pdf	

CSIRT informa phishing para validar un falso paquete de Correos de Chile	
Alerta de seguridad cibernética	8FPH22-00469-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2022
Última revisión	28 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
hXXp://www.ppinpai[.]com//vendor/phpunit/phpunit/src/Util/PHP/dazi/index/index.html	
IP	
[116.213.41.138]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00469-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00469-01.pdf	

Malware

CSIRT advierte campaña de malware Emotet	
Alerta de seguridad cibernética	2CMV21-00270-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de enero de 2022
Última revisión	28 de enero de 2022
Indicadores de compromiso	
SHA256	
f38c47db5e8cbe464420b1dc513e6d297b370286a01ebd018090e0dbfbca5161 6be929cec30a2fd7f2763adcf7cae0117df981a354180aa18269ea4575c28370 41d0933502b68fc06cbd8d872cec567a2cc8bd91b6b65ec85efe027c0ff36670	
IoC URL	
hXXp://91.240.118.168/oo/aa/se.html hXXp://91.240.118.168/oo/aa/se.png hXXp://89.184.68.240/edh2fa/g2Q7Qbgs/ hXXp://107.190.142.107/cgi-bin/hfpv/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00270-01/	
https://www.csirt.gob.cl/media/2022/01/2CMV22-00270-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades en Apple iOS y iPadOS	
Alerta de seguridad cibernética	9VSA22-00566-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2022
Última revisión	31 de enero de 2022
CVE	
CVE-2022-22584 - CVE-2022-22578 - CVE-2022-22585 CVE-2022-22587 - CVE-2022-22593 - CVE-2022-22579 CVE-2022-22589 - CVE-2022-22590 - CVE-2022-22592 CVE-2022-22594	
Fabricante	
Apple	
Productos afectados	
iPhone 6s y posteriores, iPad Pro (todos los modelos), iPad Air 2 y posteriores, iPad de 5ª generación y posteriores, iPad mini 4 y posteriores, y iPod touch (7ª generación).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00566-01/	
https://www.csirt.gob.cl/media/2022/01/9VSA22-00566-01.pdf	

CSIRT comparte vulnerabilidad en Samba	
Alerta de seguridad cibernética	9VSA22-00567-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Bajo
TLP	Blanco
Fecha de lanzamiento original	31 de enero de 2022
Última revisión	31 de enero de 2022
CVE	
CVE-2021-44141	
Fabricante	
Samba	
Productos afectados	
1.9.16, 1.9.17, 1.9.18, 2.0, 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, 2.0.5a, 2.0.6, 2.0. 7, 2.0.8, 2.0.9, 2.0.10, 2.2, 2.2.0, 2.2.0a, 2.2.1, 2.2.1a, 2.2.2, 2.2.3, 2.2.3a, 2.2.4, 2.2. 5, 2.2.6, 2.2.7, 2.2.7a, 2.2.8, 2.2.8a, 2.2.9, 2.2.10, 2.2.11, 2.2.12, 2.2a, 2.18.3, 3.0, 3.0.0 , 3.0.1, 3.0.2, 3.0.2a, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.0.7, 3.0.8, 3.0.9, 3.0.10, 3.0.11, 3.0 .12, 3.0.13, 3.0.14, 3.0.14a, 3.0.15, 3.0.16, 3.0.17, 3.0.18, 3.0.19, 3.0.20, 3.0.20a, 3.0.20b, 3.0.21 , 3.0.21a, 3.0.21b, 3.0.21c, 3.0.22, 3.0.23, 3.0.23a, 3.0.23b, 3.0.23c, 3.0.23d, 3.0.24, 3.0.25, 3.0.25a, 3.0 .25b, 3.0.25c, 3.0.26, 3.0.26a, 3.0.27, 3.0.27a, 3.0.28, 3.0.28a,	

3.0.29, 3.0.30, 3.0.31, 3.0.32, 3.0.33 , 3.0.34, 3.0.35, 3.0.36, 3.0.37, 3.1, 3.1.0, 3.2, 3.2.0, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2 .6, 3.2.7, 3.2.8, 3.2.9, 3.2.10, 3.2.11, 3.2.12, 3.2.13, 3.2.14, 3.2.15,3.3, 3.3.0, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.7, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12, 3.3.13, 3.3.14, 3.3.15, 3.3.16, 3.4, 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.4.9, 3.4.10, 3.4.11, 3.4.12, 3.4.13, 3.4.14, 3.4.15, 3.4.16, 3.4.17, 3.5, 3.5.0, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.5.6, 3.5.7, 3.5.8, 3.5.9, 3.5.10, 3.5.11, 3.5.12, 3.5. 13, 3.5.14, 3.5.15, 3.5.16, 3.5.17, 3.5.18, 3.5.19, 3.5.20, 3.5.21, 3.5.22, 3.6.0, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 3.6.11, 3.6.12, 3.6.13, 3.6.14, 3.6. 15, 3.6.16, 3.6.17, 3.6.18, 3.6.19, 3.6.20, 3.6.21, 3.6.22, 3.6.23, 3.6.24, 3.6.25, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7, 4.0.8, 4.0.9, 4.0.10, 4.0.11, 4.0.12, 4.0.13, 4.0. 14, 4.0.15, 4.0.16, 4.0.17, 4.0.18, 4.0.19, 4.0.20, 4.0.21, 4.0.22, 4.0.23, 4.0.24, 4.0.25, 4.0.26, 4.1.0,4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8, 4.1.9, 4.1.10, 4.1.11, 4.1.12, 4.1. 13, 4.1.14, 4.1.15, 4.1.16, 4.1.17, 4.1.18, 4.1.19, 4.1.20, 4.1.21, 4.1.22, 4.1.23, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, 4.2.8, 4.2.9, 4.2.10, 4.2.11, 4.2.12, 4.2.13, 4.2. 14, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8, 4.3.9, 4.3.10, 4.3.11, 4.3.12, 4.3.13, 4.4.0, 4.4.0 rc4, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4 .9, 4.4.10, 4.4.11, 4.4.12, 4.4.13, 4.4.14, 4.4.15, 4.4.16, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4 , 4.5.5, 4.5.6, 4.5.7, 4.5.8, 4.5.9, 4.5.10, 4.5.11, 4.5.12, 4.5.13, 4.5.14, 4.5.15, 4.5.16, 4.6 .0, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 4.6.8, 4.6.9, 4.6.10, 4.6.11, 4.6.12 , 4.6.13, 4.6.14, 4.6.15, 4.6.16, 4.7.0, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.7.7, 4.7 .8, 4.7.9, 4.7.10, 4.7.11, 4.7.12, 4.8.0, 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.9, 4.8.10, 4.8.11, 4.8.12, 4.9.0, 4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.9.5, 4.9.6, 4.9.7, 4.9.8, 4.9.9, 4.9. 10, 4.9.11, 4.9.12, 4.9.13, 4.9.14, 4.9.15, 4.9.16, 4.9.17, 4.9.18, 4.10.0, 4.10.1, 4.10.2, 4.10.3, 4.10.4, 4.10.5, 4.10.6, 4.10.7, 4.10.8, 4.10.9, 4.10.10, 4.10.11, 4.10.12, 4.10.13, 4.10.14, 4.10.15, 4.10. 16, 4.10.17, 4.10.18, 4.11.0, 4.11.1, 4.11.2, 4.11.3, 4.11.4, 4.11.5, 4.11.6, 4.11.7, 4.11.8, 4.11.9, 4.11.10, 4.11.11, 4.11.12, 4.11.13, 4.11.14, 4.11.15, 4.11.16, 4.11.17, 4.12.0, 4.12.1, 4.12.2, 4.12.3, 4.12. 4, 4.12.5, 4.12.6, 4.12.7, 4.12.8, 4.12.9, 4.12.10, 4.12.11, 4.12.12, 4.12.13, 4.12.14, 4.12.15, 4.13.0, 4.13.1, 4.13.2, 4.13.3, 4.13.4, 4.13.5, 4.13.6, 4.13.7, 4.13.8, 4.13.9, 4.13.10, 4.13.11, 4.13.12, 4.13. 13, 4.13.14, 4.13.15, 4.13.16, 4.13.17, 4.14.0, 4.14.1, 4.14.2, 4.14.3, 4.14.4, 4.14.5, 4.14.6, 4.14.7, 4.14.8, 4.14.9, 4.14.10, 4.14.11, 4.14.12, 4.15.0, 4.15.1, 4.15.2, 4.15.3, 4.15.4
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00567-01/
https://www.csirt.gob.cl/media/2022/01/9VSA22-00567-01.pdf

CSIRT advierte vulnerabilidad en Samba	
Alerta de seguridad cibernética	9VSA22-00558-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	1 de febrero de 2022
Última revisión	1 de febrero de 2022

CVE

CVE-2021-44142

Fabricante

Samba

Productos afectados

1.9.16, 1.9.17, 1.9.18, 2.0, 2.0.0, 2.0.1, 2.0.2, 2.0.3, 2.0.4, 2.0.5, 2.0.5a, 2.0.6, 2.0. 7, 2.0.8, 2.0.9, 2.0.10, 2.2, 2.2.0, 2.2.0a, 2.2.1, 2.2.1a, 2.2.2, 2.2.3, 2.2.3a, 2.2.4, 2.2. 5, 2.2.6, 2.2.7, 2.2.7a, 2.2.8, 2.2.8a, 2.2.9, 2.2.10, 2.2.11, 2.2.12, 2.2a, 2.18.3, 3.0, 3.0.0 , 3.0.1, 3.0.2, 3.0.2a, 3.0.3, 3.0.4, 3.0.5, 3.0.6, 3.0.7, 3.0.8, 3.0.9, 3.0.10, 3.0.11, 3.0 .12, 3.0.13, 3.0.14, 3.0.14a, 3.0.15, 3.0.16, 3.0.17, 3.0.18, 3.0.19, 3.0.20, 3.0.20a, 3.0.20b, 3.0.21 , 3.0.21a, 3.0.21b, 3.0.21c, 3.0.22, 3.0.23, 3.0.23a, 3.0.23b, 3.0.23c, 3.0.23d, 3.0.24, 3.0.25, 3.0.25a, 3.0 .25b, 3.0.25c, 3.0.26, 3.0.26a, 3.0.27, 3.0.27a, 3.0.28, 3.0.28a, 3.0.29, 3.0.30, 3.0.31, 3.0.32, 3.0.33 , 3.0.34, 3.0.35, 3.0.36, 3.0.37, 3.1, 3.1.0, 3.2, 3.2.0, 3.2.1, 3.2.2, 3.2.3, 3.2.4, 3.2.5, 3.2 .6, 3.2.7, 3.2.8, 3.2.9, 3.2.10, 3.2.11, 3.2.12, 3.2.13, 3.2.14, 3.2.15,3.3, 3.3.0, 3.3.1, 3.3.2, 3.3.3, 3.3.4, 3.3.5, 3.3.6, 3.3.7, 3.3.8, 3.3.9, 3.3.10, 3.3.11, 3.3.12, 3.3.13, 3.3.14, 3.3.15, 3.3.16, 3.4, 3.4.0, 3.4.1, 3.4.2, 3.4.3, 3.4.4, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.4.9, 3.4.10, 3.4.11, 3.4.12, 3.4.13, 3.4.14, 3.4.15, 3.4.16, 3.4.17, 3.5, 3.5.0, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, 3.5.6, 3.5.7, 3.5.8, 3.5.9, 3.5.10, 3.5.11, 3.5.12, 3.5. 13, 3.5.14, 3.5.15, 3.5.16, 3.5.17, 3.5.18, 3.5.19, 3.5.20, 3.5.21, 3.5.22, 3.6.0, 3.6.1, 3.6.2, 3.6.3, 3.6.4, 3.6.5, 3.6.6, 3.6.7, 3.6.8, 3.6.9, 3.6.10, 3.6.11, 3.6.12, 3.6.13, 3.6.14, 3.6. 15, 3.6.16, 3.6.17, 3.6.18, 3.6.19, 3.6.20, 3.6.21, 3.6.22, 3.6.23, 3.6.24, 3.6.25, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.5, 4.0.6, 4.0.7, 4.0.8, 4.0.9, 4.0.10, 4.0.11, 4.0.12, 4.0.13, 4.0. 14, 4.0.15, 4.0.16, 4.0.17, 4.0.18, 4.0.19, 4.0.20, 4.0.21, 4.0.22, 4.0.23, 4.0.24, 4.0.25, 4.0.26, 4.1.0,4.1.1, 4.1.2, 4.1.3, 4.1.4, 4.1.5, 4.1.6, 4.1.7, 4.1.8, 4.1.9, 4.1.10, 4.1.11, 4.1.12, 4.1. 13, 4.1.14, 4.1.15, 4.1.16, 4.1.17, 4.1.18, 4.1.19, 4.1.20, 4.1.21, 4.1.22, 4.1.23, 4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4, 4.2.5, 4.2.6, 4.2.7, 4.2.8, 4.2.9, 4.2.10, 4.2.11, 4.2.12, 4.2.13, 4.2. 14, 4.3.0, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8, 4.3.9, 4.3.10, 4.3.11, 4.3.12, 4.3.13, 4.4.0, 4.4.0 rc4, 4.4.1, 4.4.2, 4.4.3, 4.4.4, 4.4.5, 4.4.6, 4.4.7, 4.4.8, 4.4 .9, 4.4.10, 4.4.11, 4.4.12, 4.4.13, 4.4.14, 4.4.15, 4.4.16, 4.5.0, 4.5.1, 4.5.2, 4.5.3, 4.5.4 , 4.5.5, 4.5.6, 4.5.7, 4.5.8, 4.5.9, 4.5.10, 4.5.11, 4.5.12, 4.5.13, 4.5.14, 4.5.15, 4.5.16, 4.6 .0, 4.6.1, 4.6.2, 4.6.3, 4.6.4, 4.6.5, 4.6.6, 4.6.7, 4.6.8, 4.6.9, 4.6.10, 4.6.11, 4.6.12 , 4.6.13, 4.6.14, 4.6.15, 4.6.16, 4.7.0, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.7.7, 4.7 .8, 4.7.9, 4.7.10, 4.7.11, 4.7.12, 4.8.0, 4.8.1, 4.8.2, 4.8.3, 4.8.4, 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.9, 4.8.10, 4.8.11, 4.8.12, 4.9.0, 4.9.1, 4.9.2, 4.9.3, 4.9.4, 4.9.5, 4.9.6, 4.9.7, 4.9.8, 4.9.9, 4.9. 10, 4.9.11, 4.9.12, 4.9.13, 4.9.14, 4.9.15, 4.9.16, 4.9.17, 4.9.18, 4.10.0, 4.10.1, 4.10.2, 4.10.3, 4.10.4, 4.10.5, 4.10.6, 4.10.7, 4.10.8, 4.10.9, 4.10.10, 4.10.11, 4.10.12, 4.10.13,

4.10.14, 4.10.15, 4.10. 16, 4.10.17, 4.10.18, 4.11.0, 4.11.1, 4.11.2, 4.11.3, 4.11.4, 4.11.5, 4.11.6, 4.11.7, 4.11.8, 4.11.9, 4.11.10, 4.11.11, 4.11.12, 4.11.13, 4.11.14, 4.11.15, 4.11.16, 4.11.17, 4.12.0, 4.12.1, 4.12.2, 4.12.3, 4.12. 4, 4.12.5, 4.12.6, 4.12.7, 4.12.8, 4.12.9, 4.12.10, 4.12.11, 4.12.12, 4.12.13, 4.12.14, 4.12.15, 4.13.0, 4.13.1, 4.13.2, 4.13.3, 4.13.4, 4.13.5, 4.13.6, 4.13.7, 4.13.8, 4.13.9, 4.13.10, 4.13.11, 4.13.12, 4.13. 13, 4.13.14, 4.13.15, 4.13.16, 4.14.0, 4.14.1, 4.14.2, 4.14.3, 4.14.4, 4.14.5, 4.14.6, 4.14.7, 4.14.8, 4.14.9, 4.14.10, 4.14.11, 4.15.0, 4.15.1, 4.15.2, 4.15.3, 4.15.4
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00568-01/
https://www.csirt.gob.cl/media/2022/02/9VSA22-00568-01.pdf

CSIRT informa de vulnerabilidad en Apache	
Alerta de seguridad cibernética	9VSA22-00569-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	1 de febrero de 2022
Última revisión	1 de febrero de 2022
CVE	
CVE-2021-44451	
Fabricante	
Apache	
Productos afectados	
Apache Superset hasta 1.3.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00569-01/	
https://www.csirt.gob.cl/media/2022/02/9VSA22-00569-01.pdf	

CSIRT advierte múltiples vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA22-00570-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de febrero de 2022
Última revisión	2 de febrero de 2022

CVE

CVE-2022-0462 - CVE-2022-0470 - CVE-2022-0469
CVE-2022-0468 - CVE-2022-0467 - CVE-2022-0466
CVE-2022-0465 - CVE-2022-0464 - CVE-2022-0463
CVE-2022-0461 - CVE-2022-0452 - CVE-2022-0460
CVE-2022-0459 - CVE-2022-0458 - CVE-2022-0457
CVE-2022-0456 - CVE-2022-0455 - CVE-2022-0454
CVE-2022-0453

Fabricante

Google

Productos afectados

Google Chrome: 70.0.3538.67, 70.0.3538.77, 70.0.3538.102, 70.0.3538.110, 71.0.3578.80, 71.0.3578.98, 72.0.3626.81, 72.0.3626.96, 72.0.3626.109, 72.0.3626.119, 72.0.3626.121, 73.0.3683.75 , 73.0.3683.86, 73.0.3683.103, 74.0.3729.108, 74.0.3729.131, 74.0.3729.157, 74.0.3729.169, 75.0.3770.80, 75.0.3770.90, 75.0.3770.100, 75.0.3770.142, 76.0.3809.87, 76.0.3809.100, 76,0 .3809.132, 77.0.3865.75, 77.0.3865.90, 77.0.3865.120, 78.0.3904.70, 78.0.3904.87, 78.0.3904.97, 78.0.3904.108, 79.0.3945.79, 79.0.3945.88, 79.0.3945.117, 79.0.3945.130, 80.0.3987.87 , 80.0.3987.100, 80.0.3987.106, 80.0.3987.116, 80.0.3987.122, 80.0.3987.132, 80.0.3987.149, 80.0.3987.162, 80.0.3987.163, 81.0.4044.92, 81.0.4044.113, 81.0.4044.113, 81.0.4044.122, 81.0.4044.122, 81.0.4044.122, 81.0.4044.129, 81.0 .4044.138, 83.0.4103.61, 83.0.4103.97, 83.0.4103.106, 83.0.4103.116, 84.0.4147.89, 84.0.4147.105, 84.0.4147.125, 84.0.4147.135, 85.0.4183.83, 85.0.4183.102, 85.0.4183.121, 86.0.4240.75, 86.0.4240.111, 86.0.4240.183, 86.0.4240.193, 86.0.4240.198, 87.0.4280.66, 87.0.4280.88, 87.0.4280.141, 88.0.4324.96, 88.0.4324.104, 88.0.4324.146, 88.0.4324.150, 88.0.4324.182, 88.0.4324.190, 89.0.4389.72, 89.0.4389.82, 89.0.4389.90, 89.0.4389.114, 89.0.4389.128, 90.0.4430.72, 90.0.4430.85, 90,0. 4,430.93, 90.0.4430.212, 91.0.4472.77, 91.0.4472.101, 91.0.4472.106, 91.0.4472.114, 91.0.4472.124, 91.0.4472.164, 92.0.4515.107, 92.0.4515.131, 92.0.4515.159, 93.0.4577.63, 93.0.4577.82, 94.0.4606.54, 94.0.4606.61, 94.0.4606.71, 94.0.4606.81, 95.0.4638.54, 95.0.4638.69, 96.0.4664.45, 96.0.4664.93, 96.0.4664.110, 97.0.4692.71, 97.0.4692.99141, 88.0.4324.96, 88.0.4324.104, 88.0.4324.146, 88.0.4324.150, 88.0.4324.182, 88.0.4324.190, 89.0.4389.72, 89.0.4389.82, 89.0.4389.90, 89.0.4389.114, 89.0.4389.128, 90.0.4430.72, 90.0.4430.85, 90.0.4430.93, 90.0.4430.212, 91.0.4472.77, 91.0.4472.101, 91.0.4472.106, 91.0.4472.114, 91.0.4472.124, 91.0.4472.164, 92.0.4515.107, 92.0.4515.131, 92.0.4515.159, 93,0. 4577.63, 93.0.4577.82, 94.0.4606.54, 94.0.4606.61, 94.0.4606.71, 94.0.4606.81, 95.0.4638.54, 95.0.4638.69, 96.0.4664.45, 96.0.4664.93, 96.0.4664.110, 97.0.4692.71,

97.0.4692.99141, 88.0.4324.96, 88.0.4324.104, 88.0.4324.146, 88.0.4324.150, 88.0.4324.182, 88.0.4324.190, 89.0.4389.72, 89.0.4389.82, 89.0.4389.90, 89.0.4389.114, 89.0.4389.128, 90.0.4430.72, 90.0.4430.85, 90.0.4430.93, 90.0.4430.212, 91.0.4472.77, 91.0.4472.101, 91.0.4472.106, 91.0.4472.114, 91.0.4472.124, 91.0.4472.164, 92.0.4515.107, 92.0.4515.131, 92.0.4515.159, 93,0. 4577.63, 93.0.4577.82, 94.0.4606.54, 94.0.4606.61, 94.0.4606.71, 94.0.4606.81, 95.0.4638.54, 95.0.4638.69, 96.0.4664.45, 96.0.4664.93, 96.0.4664.110, 97.0.4692.71, 97.0.4692.99107, 92.0.4515.131, 92.0.4515.159, 93.0.4577.63, 93.0.4577.82, 94.0.4606.54, 94.0.4606.61, 94.0.4606.71, 94.0.4606.81, 95.0.4638.54, 95.0.4638.69, 96.0.4664.45, 96.0.4664.93, 96.0.4664.110, 97.0.4692.71, 97.0.4692.99107, 92.0.4515.131, 92.0.4515.159, 93.0.4577.63, 93.0.4577.82, 94.0.4606.54, 94.0.4606.61, 94.0.4606.71, 94.0.4606.81, 95.0.4638.54, 95.0.4638.69, 96.0.4664.45, 96.0.4664.93, 96.0.4664.110, 97.0.4692.71, 97.0.4692.99
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00570-01/
https://www.csirt.gob.cl/media/2022/02/9VSA22-00570-01.pdf

CSIRT informe de vulnerabilidades en Apache Log4j	
Alerta de seguridad cibernética	9VSA22-00571-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	2 de febrero de 2022
Última revisión	2 de febrero de 2022
CVE	
CVE-2021-44832	
Fabricante	
Apache	
Productos afectados	
Versiones 2.0-beta7 a 2.17.0 de Apache Log4j2 (excluidas las versiones de corrección de seguridad 2.3.2 y 2.12.4). IBM Spectrum Protect Plus 10.1.0.0-10.1.9.2 Múltiples productos de NetApp incorporan Apache Log4j.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00571-01/	
https://www.csirt.gob.cl/media/2022/02/9VSA22-00571-01.pdf	

Actualidad

Ciberconsejos para proteger tus dispositivos IoT

Si al salir de tu casa utilizas dispositivos inteligentes para protegerla, es importante que sepas que también debes cuidar este tipo de equipos, ya que existen diversos riesgos a los que estamos expuestos, como por ejemplo, secuestro de los dispositivos, robo de información o problemas de privacidad.

Tanto las cámaras, relojes, cerraduras, micrófonos, entre otros aparatos, son vulnerables, por lo que es fundamental implementar medidas básicas de seguridad para resguardar los datos y evitar que los ciberdelincuentes accedan a los dispositivos que usamos para vigilar nuestro hogar.

Para que en estas vacaciones salgas aún más tranquilo, el CSIRT de Gobierno entrega una serie de recomendaciones que te enseñarán a cómo proteger tus dispositivos IoT.

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob https://www.linkedin.com/company/csirt-gob

Recomendaciones y buenas prácticas

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los antispam y sandboxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Mathias Roco
- Juan Orellana
- Cristián Acuña
- Francisco Zapata
- Cristián González
- Luis Rojas
- Bárbara Palacios
- Lorena Araya
- Rafael Díaz
- Elías Pantoja
- Daniel Troncoso
- Héctor Gallegos
- Tania Estrada
- María Paz Villena
- José Ignacio Ávila
- Hanz Sandoval
- Didye Orellana
- Jorge Molina
- Fernando González