Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

28-01-2021 | Año 3 | N°82

Boletín de Seguridad Cibernética

Semana del 21 al 27 de Enero de 2021

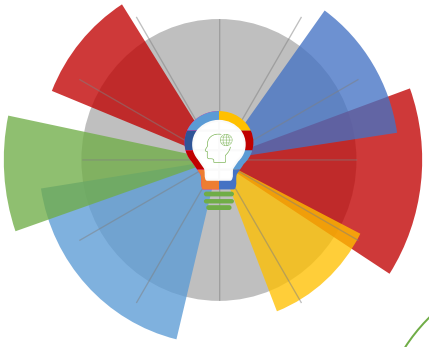
Resumen de la semana en cifras

Hash

44

Sha

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

37

URLs

Asociadas a sitios fraudulentos y campañas de phishing

Parches

63

para vulnerabilidades

Las mitigaciones son útiles para productos Terramaster, Google, Drupal, SolarWinds, Mozilla, Cisco, Apple y Liux y Unix

IPs

68

Informadas

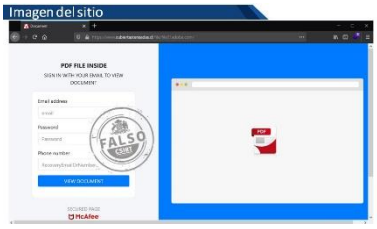
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Sitios fraudulentos

CSIRT advierte página fraudulenta de empresa de software	
Alerta de seguridad cibernética	8FFR21-00876-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Enero de 2021
Última revisión	21 de Enero de 2021
Indicadores de compromiso	
URL sitio falso	
https[:]//pathayescon[.]cl/WillamScottLaw/tcwoodinc/u.php	
IP	
186[.]64.119.145	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR21-00876-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00876-01.pdf	

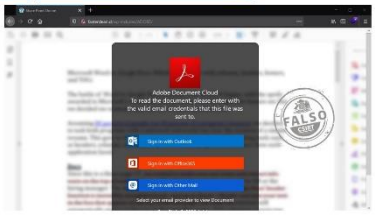


CSIRT advierte página fraudulenta de empresa de software	
Alerta de seguridad cibernética	8FFR21-00877-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Enero de 2021
Última revisión	21 de Enero de 2021
Indicadores de compromiso	
URL sitio falso	
https[:]//www.cubiertastensadas[.]cl/file/file01adobe.com/	
IP	
162[.]241.153.137	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR21-00877-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00877-01.pdf	

Imagen del sitio

CSIRT informa portal de firma electrónica falso	
Alerta de seguridad cibernética	8FFR21-00878-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2021
Última revisión	22 de Enero de 2021
Indicadores de compromiso	
URL sitio falso	
http[:]//cedarcp[.]cl/thecrowngroup/tcwoodinc/u.php	
IP	
186[.]64.118.225	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR21-00878-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00878-01.pdf	

Imagen del sitio



CSIRT informa página de software fraudulenta	
Alerta de seguridad cibernética	8FFR21-00879-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2021
Última revisión	22 de Enero de 2021
Indicadores de compromiso	
URL sitio falso	
http[:]//fasterclean[.]cl/wp-includes/ADOBE/	
IP	
66[.]232.107.218	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR21-00879-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00879-01.pdf	

CSIRT informa portal bancario fraudulento	
Alerta de seguridad cibernética	8FFR21-00880-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//cuentarutusuarios[.]cl/personas/pagina/imagenes/comun2008/banca-en-lineapersonas.html	
IP	
186[.]64.118.235]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00880-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00880-01.pdf	

CSIRT informa página de entidad bancaria falsa	
Alerta de seguridad cibernética	8FFR21-00881-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//www.bancosanta-nder[.]link/	
IP	
198[.]54.116.238	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR21-00881-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00881-01.pdf	

CSIRT informa suplantación de sitio bancario	
Alerta de seguridad cibernética	8FFR21-00882-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//santander-persona-cl.eugenedps[.]com/	
IP	
69[.]27.37.216	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8FFR21-00882-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00882-01.pdf	

CSIRT informa portal de banco fraudulento	
Alerta de seguridad cibernética	8FFR21-00883-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//www.superclave-validar-bancaporinternet[.]app	
IP	
198[.]54.126.75	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00883-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00883-01.pdf	

Imagen del sitio

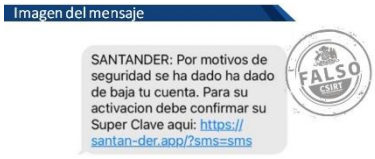
CSIRT advierte página fraudulenta bancaria	
Alerta de seguridad cibernética	8FFR21-00884-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//www.bancosant-ander[.]app/	
IP	
198[.]54.126.76	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00884-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00884-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing con supuesta renovación de tarjeta	
Alerta de seguridad cibernética	8FPH21-00358-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2021
Última revisión	22 de Enero de 2021
Indicadores de compromiso	
URL redirección	
https://bit[.]ly/3bRVu3e?l=www.bancoestado.cl	
URL sitio falso	
http://ashkkosar[.]ir/cli/www.bancoestado.cl/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
69[.]16.226.142	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00358-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00358-01-1.pdf	

Imagen del mensaje



CSIRT advierte smishing de supuesta cuenta dada de baja	
Alerta de seguridad cibernética	8FPH21-00359-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2021
Última revisión	22 de Enero de 2021
Indicadores de compromiso	
URL redirección	
https://santan-der[.]app/?sms=sms	
URL sitio falso	
https://santand-ercl[.]app/1611335805/personas/index.asp	
IP	
198[.]54.126.77	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00359-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00359-01-1.pdf	

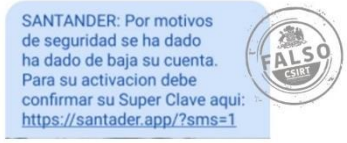
Imagen del mensaje

CSIRT informa smishing de tarjeta bloqueada	
Alerta de seguridad cibernética	8FPH21-00360-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2021
Última revisión	25 de Enero de 2021
Indicadores de compromiso	
URL redirección	
https[:]//santader-sms[.]app/?sms=santander	
URL sitio falso	
https[:]//bancosantan-der[.]live/1611601036/personas/index.asp	
IP	
198[.]54.115.246	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00360-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00360-01-1.pdf	

Imagen del mensaje

CSIRT advierte phishing de bloqueo de cuenta	
Alerta de seguridad cibernética	8FPH21-00361-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2021
Última revisión	25 de Enero de 2021
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/2LM7GrO?l=www.santander[.]cl	
http[:]//wordpress.roma[.]it/favicon/enviar03.php?l=1192449359	
URL sitio falso	
http[:]//ashkkosar[.]ir/media/www.santander.cl/pagina/login.asp	
IP	
207[.]182.140.101	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00361-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00361-01.pdf	

Imagen del mensaje



CSIRT CSIRT advierte smishing de cuenta desactivada	
Alerta de seguridad cibernética	8FPH21-00362-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
URL redirección	
https[:]//santader[.]app/?sms=1	
URL sitio falso	
https[:]//superclave-validar-bancaporinternet[.]app/1611762370/personas/index.asp	
IP	
198[.]54.126.75	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00362-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00362-01.pdf	

Malware


Imagen del mensaje

Buenos días

Aquí encontrará nuestro pedido PO-#7507 para su acción rápida.

Envíe su presupuesto para el siguiente artículo:

DAR HOJA DE DATOS / DIBUJO PARA EL MISMO PRESUPUESTO

POR FAVOR QUOTE CONSULTE ATAQUE PARA MAS INFORMACION Y DÁNOS UN PRECIO EXACTO

No dude en ponerse en contacto con nosotros si necesita más claridad.

Gracias & Saludos

D. Rodriguez
Departamento de Adquisiciones | ALCEDA SA DE CV
TEL: (33) 3587 5440 FAX: (33) 3587 5439
EMAIL: d.garzarodriguez@alceda.com.mx

CSIRT advierte campaña de malware con supuesto presupuesto	
Alerta de seguridad cibernética	2CMV21-00139-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
Indicadores de compromiso	
SHA256	
5B49A5C0C5948F944B9C80773DD2E6958B320ED31934F265B509570563A89545	
7B65D3923CBFFAD3828DCAD9E9BF7B107CC2F3041CF965EBD3FBE730FC6302FE	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv21-00139-01/	
https://www.csirt.gob.cl/media/2021/01/2CMV21-00139-01.pdf	

Vulnerabilidades

CSIRT CSIRT advierte vulnerabilidades que afectan a TerraMaster TOS	
Alerta de seguridad cibernética	9VSA21-00369-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Enero de 2021
Última revisión	21 de Enero de 2021
CVE	
CVE-2020-28184 - CVE-2020-28185 - CVE-2020-28186 CVE-2020-28187 - CVE-2020-28188 - CVE-2020-28189 CVE-2020-28190	
Fabricante	
TerraMaster	
Productos afectados	
TerraMaster TOS 4.2.06.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00369-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00369-01.pdf	

CSIRT comparte vulnerabilidades que afectan a Google Chrome	
Alerta de seguridad cibernética	9VSA21-00370-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Enero de 2021
Última revisión	21 de Enero de 2021
CVE	
CVE-2021-21134 - CVE-2021-21128 - CVE-2021-21129 CVE-2021-21130 - CVE-2021-21131 - CVE-2021-21132 CVE-2021-21133 - CVE-2021-21135 - CVE-2021-21126 CVE-2021-21136 - CVE-2021-21137 - CVE-2021-21138 CVE-2021-21139 - CVE-2021-21140 - CVE-2021-21141 CVE-2021-21127 - CVE-2021-21125 - CVE-2021-21124 CVE-2021-21117 - CVE-2021-21118 - CVE-2021-21119 CVE-2021-21120 - CVE-2021-21121 - CVE-2021-21122 CVE-2021-21123 - CVE-2020-16044	
Fabricante	
Google	
Productos afectados	
Google Chrome, versiones de la 88.0.4324.0 a la 88.0.4324.95.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00370-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00370-01.pdf	

CSIRT comparte mitigaciones obtenidas de Drupal	
Alerta de seguridad cibernética	9VSA21-00371-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2021
Última revisión	22 de Enero de 2021
CVE	
CVE-2020-36193	
Fabricante	
Drupal	
Productos afectados	
Archive_Tar, versiones de la 0.3 a la 1.4.11.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00371-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00371-01.pdf	

CSIRT advierte vulnerabilidades entregadas por SolarWinds	
Alerta de seguridad cibernética	9VSA21-00372-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de Enero de 2021
Última revisión	22 de Enero de 2021
CVE	
CVE-2020-27871 - CVE-2020-27870 - CVE-2020-27869 CVE-2020-14005	
Fabricante	
SolarWinds	
Productos afectados	
Orion Platform, versiones de la 2019.2 a la 2020.2.1 HF 1. Orion Network Performance Monitor, versiones de la 2019.4 a la 2020.2 Hotfix 1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00372-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00372-01.pdf	

CSIRT comparte vulnerabilidades de Chromium y Google Chrome	
Alerta de seguridad cibernética	9VSA21-00373-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2021
Última revisión	25 de Enero de 2021
CVE	
CVE-2020-16044 - CVE-2021-21117 - CVE-2021-21118 CVE-2021-21119 - CVE-2021-21120 - CVE-2021-21121 CVE-2021-21122 - CVE-2021-21123 - CVE-2021-21124 CVE-2021-21125 - CVE-2021-21126 - CVE-2021-21127 CVE-2021-21128 - CVE-2021-21129 - CVE-2021-21130 CVE-2021-21131 - CVE-2021-21132 - CVE-2021-21133 CVE-2021-21134 - CVE-2021-21135 - CVE-2021-21136 CVE-2021-21137 - CVE-2021-21138 - CVE-2021-21139 CVE-2021-21140 - CVE-2021-21141	
Fabricante	
Gentoo	
Productos afectados	
Chromium y Google Chrome, versiones anteriores a 88.0.4324.96.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00373-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00373-01.pdf	

CSIRT advierte vulnerabilidad de Mozilla Thunderbird	
Alerta de seguridad cibernética	9VSA21-00374-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Enero de 2021
Última revisión	25 de Enero de 2021
CVE	
CVE-2020-16044	
Fabricante	
Mozilla	
Productos afectados	
Mozilla Thunderbird hasta la versión 78.6.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00374-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00374-01.pdf	

CSIRT comparte mitigaciones obtenidas de Cisco	
Alerta de seguridad cibernética	9VSA21-00375-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de Enero de 2021
Última revisión	26 de Enero de 2021

CVE

CVE-2021-1264 - CVE-2021-1257 - CVE-2021-1265
CVE-2021-1138 - CVE-2021-1139 - CVE-2021-1140
CVE-2021-1141 - CVE-2021-1142 - CVE-2021-1241
CVE-2021-1273 - CVE-2021-1274 - CVE-2021-1278
CVE-2021-1279 - CVE-2021-1302 - CVE-2021-1304
CVE-2021-1305 - CVE-2021-1218 - CVE-2021-1259
CVE-2021-1300 - CVE-2021-1301

Fabricante

Cisco

Productos afectados

CVE-2021-1264: Cisco DNA Center, versiones anteriores a la 1.3.1.0.
CVE-2021-1257 y CVE-2021-1265: Cisco DNA Center, versiones anteriores a la 2.1.1.0.
CVE-2021-1138, CVE-2021-1139, CVE-2021-1140, CVE-2021-1141 y CVE-2021-1142: Cisco Smart
Software Manager Satellite, versiones anteriores a la 6.3.0. (desde la cual el producto fue
renombrado como Cisco Smart Software Manager On-Prem).
CVE-2021-1241: Cisco SD-WAN (versiones 18.3.0 a 20.4.0), routers Cisco SD-WAN vEdge.
CVE-2021-1273: Cisco SD-WAN (versiones 18.3.0 a 20.4.0), Cisco SD-WAN vBond Orchestrator, Cisco
SD-WAN vEdge Cloud Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage y Cisco SD-WAN
vSmart Controller.
CVE-2021-1274: Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud Router, routers Cisco
SD-WAN vEdge, Cisco SD-WAN vManage, Cisco SD-WAN vSmart Controller, y los Cisco IOS XE SD-WAN
anteriores a la version 16.12.4.
CVE-2021-1278 y CVE-2021-1279: Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud
Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage, Cisco SD-WAN vSmart Controller, y los
Cisco SD-WAN versiones de la 18.3.0 a la 20.3.0.
CVE-2021-1300 y CVE-2021-1301: Cisco SD-WAN vBond Orchestrator, Cisco SD-WAN vEdge Cloud
Router, routers Cisco SD-WAN vEdge, Cisco SD-WAN vManage, Cisco SD-WAN vSmart Controller,
Cisco IOS XE SD-WAN, versiones hasta la 16.12 y los Cisco SD-WAN versiones

de la 18.3.0 a la 20.3.0. CVE-2021-1302, CVE-2021-1304 y CVE-2021-1305: Cisco SD-WAN vManage, versiones de la 18.3 a la 20.4.0. CVE-2021-1218: Cisco Smart Software Manager Satellite: 5.0 CVE-2021-1259: Cisco SD-WAN vManage, versiones anteriores a la 18.2.0.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00375-01/
https://www.csirt.gob.cl/media/2021/01/9VSA21-00375-01.pdf

CSIRT comparte vulnerabilidades entregadas por Apple	
Alerta de seguridad cibernética	9VSA21-00376-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
CVE	
CVE-2021-1782 - CVE-2021-1870 - CVE-2021-1871	
Fabricante	
Apple	
Productos afectados	
iPhone 6 y posteriores iPad Air 2 y posteriores iPad mini 4 y posteriores Apple TV 4K Apple TV HD	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00376-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00376-01.pdf	

CSIRT comparte mitigación para los sistemas Linux y Unix	
Alerta de seguridad cibernética	9VSA21-00377-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
CVE	
CVE-2021-3156	
Fabricante	
Sudo	
Productos afectados	
Sistemas operativos basados en Unix y Linux que usen Sudo, versiones legado hasta la 1.8.2 y 1.8.31p2, y todas las versiones estables de la 1.9.0 a 1.9.5p1 en su configuración por defecto.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00377-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00377-01.pdf	

CSIRT comparte vulnerabilidad entregada por SonicWall	
Alerta de seguridad cibernética	9VSA21-00378-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	27 de Enero de 2021
Última revisión	27 de Enero de 2021
CVE	
CVE Pendiente	
Fabricante	
SonicWall	
Productos afectados	
SMA 100 Series (SMA 100, SMA 210, SMA 400, SMA 500v).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00378-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00378-01.pdf	

IoC Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos
5a17dee61b79152ce451f560a17603b291bd0934b4c0bdb69a3328fca8b36771
743b0489a94f04569f1dd9ea1c62d1d5d6ce22b642369e87f974b3635990edb8
11e1780e215a952185315253632033b1e42e269f59252e80ccc002e7ed15c086
c4f94c6960792fe6e062b42c6c149482152a96588a9a5b9c3f7c4a35c974ac50
4142cfc2bb8a067a21c0439bef1d08e1742025b00b3cb1c9619ff7bf0a2b42d6
1fa18e851ad74226caf71eaca19ccba3ba2b1457521c4a4fbe6ba07fb3008333
17420055c7c1b85137e8f5e78a7eab811ae1b4f00b33ce05590e19399286fe2f
fb4541bb676e36bc08711601b21c85ec6a0eec67fa65a2ac53a7e70a8f01c628
75d4b326ca471055fba9d3e4dfbb994e191135130d15f7f1e75fa6a8346bf89d
1b2b0f6f229f819f49cefa1af565aa4e83bf8b1f9df047bebfa9143dbebbb349
51d0ab773047ebaac512a5d397e79534ac5b266afd4ee691d6356a8bd7fe4b11
3602f8e737829acb355fceaf51908fe8a199a2ae44099cedd08d3cb298fc8b53
58bd78843e708ee76feee70fd020e5e0ff29c4ad4df2aebbd48ca6d587b15912
0f0061b80732fc11150a67c1807a75989ce897eb2be6e22d425c4b41f88f98ee
c84de615620cd1a69411f262b2f431ac07909b7705e43c1a97d80f5bfdc3ea33
57c0a7e0c8c758419617cbb0493789572ffd9bad491e5e98ecb0754de052efe3
fafa1cf428d6c5e3cc4e6538a098ed38e2ffbd8c9dc5ea06313648aafe2fa0a4
5f6d69e58850b0965c708c5e8cbf7f3f0a769a42c33abe4a82595f903ad92dbe
922d235666c1b57e9aff2834a273334b7e72c3963d98f1a4d8d02287c540a997
849af1e2dd0cefe909b1e37a24266f716af4687eab7ace3bb9bc28c921c4f999
a6b87278bb77d9a04427862b72b0c109e770f31d1c6c6da47644a2dbd82cad11
fcb1b3759243a11409e9c374d7feef2bd785139f1871e23eb04a745e492b0d84
0ded59b8e793df139715fe181350639f9f92855d28917d5321a8c7ee5ca178dd
13fa691fa4a6d36f4aa041d3159233a3272fe9d6a2837dfafa1a34235833221b
8a4ec0ca950a390ef42dca2eba4cb2baea9d9239ab969b07b0596fa2e601e01c
bd207412e6350e4c7e0f4149a5e2e5f607193dbd98360ec8e696ef42cd6ba4ad
3fe9826f416743be9ec86023808b246c046a0384db9c9c81268ce8fd008c792d
24ff39d73f1df07521eae970f57ccb4c214adec5a1a9e3941890abea7f59810b
4d972e37eedaf19d2f0e71ed55568cce27b0860e54906c5442ca69c2e2f0d360

54accdc2c15133ddabb1dd67159f363044ec299963688259f2947ef9b8160093
f773095273ff78e1678a13fcec9c17b2cce0412f13c0f12e09cdd6173ffc82c3
93c786b73d5a68527bfa3630ed9578fa6706cc9be21c746852baf913281825e2
ad2d3f962576e50cdece1884fb9584e0b6269c551eafe565e3062ff01b2b33b9
225dada2c55351dee296d9491814c30a9d0e2ddfaeaa742ae6e65c1373cf7006
49308d0126ffd48ff35716a5ae47551d1f438df17fd32fb704f9f4c4ecf0a204
e3a69d01de9b2730ba45903580e9e6a0add7228fdf3f1e63afae1154d10e2994
e785b9df7a3848de00d34c09968f29b9a60d2bc99d0a67b743beda66ecc1e534
30d2ab012c781742249e962105127383ca1a9511ee31e37ae9679156c8678414
4dc0440cf9d2fcf0be2a006dc6576fd946a71e0e18d826dfd2e458e8d3b03b3f
6704fb0e9569d0bf2fb207c045fae37fa2213f02a526678f2b09dbb608856cfa
86eb6cb673d76cf76312c584873effd76c4a12f73c98188e43a5e50aded5b381
b5c32583f3b2d083f603c516afef770c77e5b353a5972a3fa728dfb9bb8b352a

Correos electrónicos de donde son enviados los archivos adjuntos con malware

silvia.almaraz@loubet.com.mx
christian.sagadraca@nfc.gov.ph
visas2@siecindia.com
vikki.tambe@sysnetglobal.com
dnduw@nduwsfamily.com
ych512@ms75.hinet.net
asif@regrowz.in
gemma.miaventilation@miachina.net
walaa@metrofiresystems.com
pedidos@laveiga.com
zahid@roshnimm.com
sherrera@makler.com.ve
jean-yves.lameyse@paris.notaires.fr
ehernandez@decimas.es
finance@pinstarauto.com
mail@libertylease.nl
seiaprod@seia.cl
3d@threenarrewarren.com.au
info@caa-ingenieria.com.ar
toanbui@benhvienranghammat.vn
submission@najmedicine.us
info@turismoproclusone.it

esperanza@protools.mx
progettazione.p@rossini1969.it
accounts@stopl.in
n.gouveia@qualiconsig.com.br
spg@spgbrindisi.it
ruben@granimarloranca.com
branchmanager.skp@shaheen-traders.com
r_kakita@hamaoka-industry.com
compras@josehuespeehijos.com.ar
Samiuddinr@hotmail.com
SHALEY.NG@ienergy.com.sg
recruitment@shengtai.co.th
radeivanovic@dmdm.rs
edi@taiheidenki.co.jp
f.kondoh@eiwa-bussan.com
onestcool@aei.ca
suzuki@ekouwa.co.jp
marketing@oldtile.com.my
whybrta.control@wernerco.com
office@metreoxporters.net
tr@purfactory.pw
commerciale@tecnomill.net
accounts@primaryfreight.com
regulatory@hds.com.jo

Direcciones IP de servidor SMTP donde es enviado el correo malicioso: Recomendamos establecer cuarentena preventiva para estos indicadores de compromiso, previa evaluación del impacto en los servicios productivos. Una vez que sus plataformas de monitoreo no detecten actividad maliciosa, puede evaluar la posibilidad de liberar el bloqueo. Es importante considerar que podrían aparecer direcciones de IP de servicios Cloud reconocidos o amenazas mitigadas.

69.89.20.226
192.185.50.93
216.10.244.214
172.104.61.201
168.95.4.114
162.210.70.184
162.210.70.2

162.251.83.181
175.107.198.7
50.116.124.69
170.249.199.130
162.252.57.42
114.31.72.17
207.21.192.5
103.45.230.198
103.120.176.28
62.149.157.213
62.149.157.212
62.149.157.215
198.71.225.36
69.89.29.114
201.76.49.59
62.149.156.87
62.149.158.132
69.89.25.95
62.149.157.216
62.149.157.214
219.99.187.7
189.126.112.61
181.31.135.145
193.56.28.234
217.74.103.244
116.202.193.189
145.131.7.81
79.101.22.73
153.138.238.39
153.138.238.41
153.149.228.33
153.149.228.36
153.149.232.32
153.153.67.33
153.138.238.38
153.153.67.35
153.138.237.38

153.153.67.34
206.123.6.133
202.191.118.236
160.20.147.181
23.227.199.25
94.198.40.46
104.168.144.234
154.16.67.6
103.141.138.130
185.222.57.238

IoC Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el fin de suplantar un remitente original y así depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP
78.128.113.66
212.70.149.54
212.70.149.85
5.188.206.204
37.49.225.207
141.98.80.101
72.11.135.222
193.105.134.232
190.21.158.16

Actualidad

Cibersucesos n°6

CSIRT presenta una nueva edición de Cibersucesos, publicación que dedicamos a la Transformación Digital. Como tema central de esta edición, tenemos un análisis de la importancia de llevar a cabo una transformación digital que tenga como requisito y norte la ciberseguridad. Para esto, es primordial desarrollar y mantener una arquitectura de red segura, que tenga en mente la proliferación del denominado internet de las cosas, los mecanismos para que exista una autentificación eficaz de los usuarios, y lograr una alta disponibilidad e interoperabilidad de los sistemas, entre otros factores.

La sección de Cooperación Internacional presenta este número a Estonia, país líder mundial en la digitalización de su relación entre el Estado y los ciudadanos. La experiencia de esta nación báltica, que recién este año cumple 30 años desde su independencia de la Unión Soviética, implementando una revolucionaria infraestructura de identidad digital, es descrita en detalle por dos expertas de la Autoridad de Sistemas de Información de Estonia.

En Tendencias, presentamos (como no podía ser de otra forma para la primera edición del año), las principales técnicas que deberían "ponerse de moda" entre los ciberdelincuentes durante 2021, junto asimismo con nuevas tecnologías que podrían ayudar a mejorar nuestras defensas. La sección Comunidad Hacker cuenta en esta ocasión con la Fundación País Digital, que nos aconseja y explica las formas en que apoyan a las pymes para generar un proceso de transformación digital exitoso, incluyendo seminarios y talleres para la entrega a las pequeñas empresas de los conocimientos necesarios para esta transformación, además de una herramienta de chequeo para que puedan diagnosticar su nivel de madurez digital.

Ver más: https://bit.ly/3gO8ab9

Superintendencia de Casinos de Juego publica consulta sobre normativa para la gestión de la seguridad de la información

Como resultado de la cooperación con el CSIRT de Gobierno, la Superintendencia de Casinos de Juego publicó la circular que establece los criterios que deberán seguir las empresas del sector para la gestión de la información e implementación de la ciberseguridad. La recepción de comentarios concluye el 5 de febrero.

Un importante avance en materia de ciberseguridad concretó la Superintendencia de Casinos de Juego (SCJ). Eso porque dio a conocer, a través de su sitio web y para consulta pública, la circular que fija los estándares y normativas para la gestión de la información, gracias a un trabajo en conjunto con el Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno.

Este futuro marco regulatorio entrega instrucciones tanto para la gestión de la información como de la ciberseguridad. Así, el documento busca entregar a todas las entidades que dependan de la SCJ los reglamentos generales de ciberseguridad que deben considerar como lineamientos mínimos a cumplir. El plazo de recepción de comentarios por parte de la comunidad es el 5 de febrero de 2021.

Algunos de los puntos que aborda la normativa en materia de ciberseguridad son:

- Gestión del riesgo: Analizar el impacto operacional de los riesgos, establecer controles para la mitigación de los mismos y definir el ciclo de vida de un incidente. Por lo tanto, considera la prevención, detección, análisis, notificación, contención, radicación, recuperación, documentación del incidente y su escalamiento a las instancias respectivas.
- Prevención y gestión de la ciberseguridad: Se proponen definiciones comunes, ya que el ecosistema digital es uno solo, y el objetivo es que todas las instituciones adquieran el mismo lenguaje respecto, por ejemplo, a los incidentes.
- Criterios para notificar: Establece estándares comunes para determinar el tipo y nivel peligrosidad e impacto de los incidentes. Se deberá notificar si los incidentes son de riesgo grave, muy alto y alto.
- Canales o vía de notificación: Se fija la manera en que se comunicarán los incidentes. Además, se deberá nombrar a una contraparte, un encargado suplente y un equipo de respuesta.

Para conocer más sobre esta consulta pública, puedes ingresar a

http://www.scj.gob.cl/marco-normativo/normativas-en-consulta/circular-de-ciberseguridad

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- 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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- José Gastón Muñoz
- Jaime Andrés Munita
- Claudio Valderrama
- Cristóbal Herrera
- Felipe Zura Rojas
- Rodrigo González Azolas (CompuNet)

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.29 15:47:10 -03'00'