Ministerio del Interior y Seguridad Pública

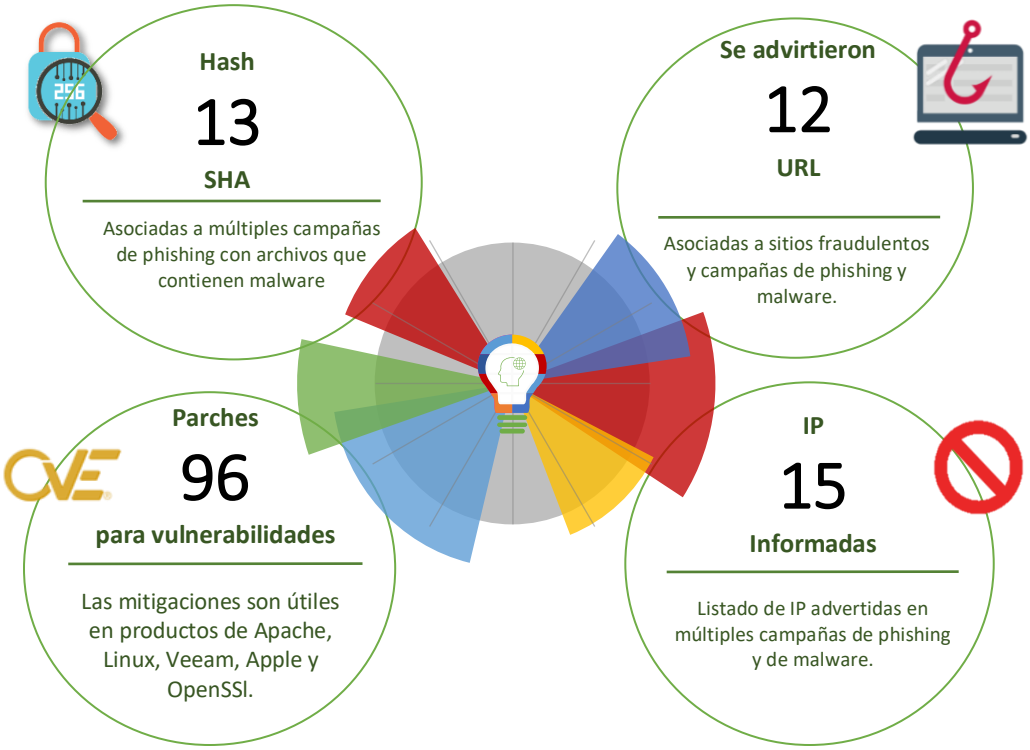
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

18-03-2022 | Año 4 | N°141

Boletín de Seguridad Cibernética

Semana del 11 al 17 de marzo de 2021

La semana en cifras



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

Contenido

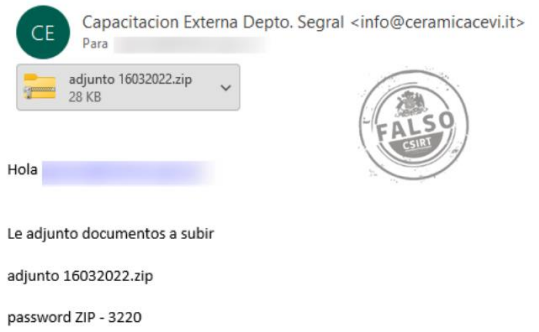
https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
https://www.linkedin.com/company/csirt-gob

Malware

Imagen del mensaje

CSIRT alerta campaña de malware con falso pedido	
Alerta de seguridad cibernética	2CMV21-00282-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2021
Última revisión	15 de marzo de 2021
Indicadores de compromiso	
SHA256	
382DB49B891A9D2DF05CE4CA1335868FA3CFF3896CA905D56C84BAA5B28371B0 A84BDF209B862FFBDF3D963611EEC3C1C2D70024E24041727A49BC618D6FF4CD	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0282-01/ https://www.csirt.gob.cl/media/2022/03/2CMV22-00282-01.pdf	

Imagen del mensaje



CSIRT advierte campaña con malware con falso documento	
Alerta de seguridad cibernética	2CMV21-00283-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2021
Última revisión	15 de marzo de 2021
Indicadores de compromiso	
SHA256	
E22856F85636FD54CB7DFD60484C1B1D9D6DD0237C7582597DCF2D51EB42C8A5 50E669DCF64DEDAF5F6FA5663134B3C2A0261B5107BF292DBBAC6C6650458439 BF6A325D9C610EE47E88FA32A5FE24468E37A6C7894F3CCC98CC7E2D76DB27A5 6F1D9EADEB217CCEB92C369A01CCC1057760EB92741A5D0B25742B50CCA9C9B4 6A80A236C7CF8F852B2ED1B42FF6387F7B014909631E79A2DFBBF766301A309E 56494BC247FB5AC665B921664B9207CB40BF3A8E6C91F3A8AAB078A06ADD64EA 58DCADB039E985C7777D78E8968DF9A2671332AE233537FC6279AA6E23461155 01839B30AFA4875CFE1891B903F4C6A46D8D78F085CAF638F5CF8A7A38B97964 2E785E93340BEF5E64E8AEC5A817BC676EB6757412574059894ED700ACF42909	
IoC URL	
http://suleyera[.]com/components/CNGhltc5v2K6 http://sociallysavvyseo[.]com/PinnacleDynamicServices/pRlYMzvf uu5B/ http://moveit.savvyint[.]com/config/DsfssbO7BYG/ https://schwizer.net/styled/D0MG/ http://shabeerpv.atwebpages[.]com/css/ww6if1YAsMpjpuGz http://shimal.atwebpages[.]com/wp-content/xkaRkHr/	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0283-01/ https://www.csirt.gob.cl/media/2022/03/2CMV22-00283-01.pdf	

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

Imagen del mensaje

CSIRT alerta campaña de malware que suplanta a la Tesorería General de la República	
Alerta de seguridad cibernética	2CMV21-00284-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de marzo de 2021
Última revisión	16 de marzo de 2021
Indicadores de compromiso	
SHA256	
5C4E6F90364DFEB19C1E7EA55B516F8BA211B2DCE1FF4F93B7C8DD32A61F2CC6 85EB1D4FD5DC78552361BB1DA4422C0865BBAE3784470C2FAA551E461FB35D52	
IoC URL	
https://5aa20a4eab0b.ngrok[.]io/PDF-0027430505S3B101lF3.zip https://makeupkala[.]com/well-known/acme-challenge/l/z/c218B3505l1016S502i3.zip https://zakatalquds[.]org/profiles/contts/hd218b0s5S20d1l322cj.php	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-0284-01/ https://www.csirt.gob.cl/media/2022/03/2CMV22-00284-01.pdf	

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

Phishing

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00481-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de marzo de 2022
Última revisión	18 de marzo de 2022
Indicadores de compromiso	
URL redirección	
https://www.csc-solutions.eu/wp-content/themes/--/Bloqueio_Tarjeta/?cliente=	
URL sitio falso	
https://email1.portabilidad-tarjeta[.]com/control.php	
IP	
[212.192.246.72]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00481-01/	
https://www.csirt.gob.cl/media/2022/03/8FPH22-00481-01.pdf	

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

Sitios fraudulentos

Imagen del sitio

CSIRT advierte sitio web que suplanta a radio Cooperativa	
Alerta de seguridad cibernética	8FFR22-01063-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de marzo de 2022
Última revisión	16 de marzo de 2022
Indicadores de compromiso	
URL sitio falso	
https://flexibleme[.]xyz/santa-monica	
IP	
[104.21.21.250]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01063-01/	
https://www.csirt.gob.cl/media/2022/03/8FFR22-01063-01.pdf	

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

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	Nombre sistema autónomo	Documento web
177.53.165.206	Provarp informatica	4IIA22-00049-01
170.254.160.97	Companhia itabirana telecomunicacoes ltda	4IIA22-00049-01
103.25.132.125	Five network broadband solution pvt ltd	4IIA22-00049-01
168.0.252.14	Afinet solucoes em tecnologia da informacao ltda	4IIA22-00049-01
45.176.215.137	Erbcom telecomunicacoes eireli – me	4IIA22-00049-01
103.119.78.238	Speed4net	4IIA22-00049-01
175.176.185.122	Netplus broadband services private limited	4IIA22-00049-01
103.59.135.252	Ero wide comm private limited	4IIA22-00049-01
45.6.27.220	Daltony carlos tavares caetano munhoz me	4IIA22-00049-01
179.127.195.130	Afinet solucoes em tecnologia da informacao ltda	4IIA22-00049-01
168.194.154.129	Imax wireless provedor de internet ltda	4IIA22-00049-01
131.196.95.62	Global telecom do brasil	4IIA22-00049-01
89.186.5.226	Artur sienkiewicz	4IIA22-00049-01

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

Vulnerabilidades

CSIRT advierte vulnerabilidades en Apache HTTP Server	
Alerta de seguridad cibernética	9VSA22-00591-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de marzo de 2022
Última revisión	14 de marzo de 2022
CVE	
CVE-2022-23943 CVE-2022-22721 CVE-2022-22720 CVE-2022-22719	
Fabricante	
Apache	
Productos afectados	
Servidor Apache HTTP: 2.4.0 – 2.4.52	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00591-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00591-01.pdf	

CSIRT comparte vulnerabilidades en el kernel de Linux	
Alerta de seguridad cibernética	9VSA22-00592-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de marzo de 2022
Última revisión	14 de marzo de 2022
CVE	
CVE-2022-25636	
Fabricante	
Varios, que basan sus productos en el kernel de Linux	
Productos afectados	
Linux 5.4 a 5.6.10 Red Hat: Este problema afecta los paquetes del kernel de Linux enviados con Red Hat Enterprise Linux 8.3 GA en adelante. Las versiones anteriores de Red Hat Enterprise Linux no se ven afectadas. Productos SUSE: SUSE Linux Enterprise Desktop 15 SP3	

SUSE Linux Enterprise Informática de alto rendimiento 15 SP3 Módulo SUSE Linux Enterprise para el sistema base 15 SP3 Módulo SUSE Linux Enterprise para herramientas de desarrollo 15 SP3 Módulo SUSE Linux Enterprise para la nube pública 15 SP3 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server para aplicaciones SAP 15 SP3 Administrador de SUSE Proxy 4.2 Servidor SUSE Manager 4.2 SUSE Módulo en tiempo real 15 SP3 Versiones Debian: 5.10.84-1 5.10.103-1 5.16.11-1
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00592-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00592-01.pdf

CSIRT advierte vulnerabilidades en Veeam Backup & Replication	
Alerta de seguridad cibernética	9VSA22-00593-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2022
Última revisión	15 de marzo de 2022
CVE	
CVE-2022-26500 CVE-2022-26501 CVE-2022-26504	
Fabricante	
Veeam	
Productos afectados	
Servidor Apache HTTP: 2.4.0 – 2.4.52	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00593-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00593-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en productos de Apple	
Alerta de seguridad cibernética	9VSA22-00594-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2022
Última revisión	15 de marzo de 2022

CVE

CVE-2019-14379	CVE-2022-22607	CVE-2022-22638
CVE-2021-22945	CVE-2022-22608	CVE-2022-22639
CVE-2021-22946	CVE-2022-22609	CVE-2022-22640
CVE-2021-22947	CVE-2022-22610	CVE-2022-22641
CVE-2021-30918	CVE-2022-22611	CVE-2022-22642
CVE-2021-36976	CVE-2022-22612	CVE-2022-22643
CVE-2021-4136	CVE-2022-22613	CVE-2022-22644
CVE-2021-4166	CVE-2022-22614	CVE-2022-22647
CVE-2021-4173	CVE-2022-22615	CVE-2022-22648
CVE-2021-4187	CVE-2022-22616	CVE-2022-22650
CVE-2021-4192	CVE-2022-22617	CVE-2022-22651
CVE-2021-4193	CVE-2022-22618	CVE-2022-22652
CVE-2021-44228	CVE-2022-22621	CVE-2022-22653
CVE-2021-46059	CVE-2022-22622	CVE-2022-22654
CVE-2022-0128	CVE-2022-22623	CVE-2022-22656
CVE-2022-0156	CVE-2022-22624	CVE-2022-22657
CVE-2022-0158	CVE-2022-22625	CVE-2022-22659
CVE-2022-22582	CVE-2022-22626	CVE-2022-22660
CVE-2022-22596	CVE-2022-22627	CVE-2022-22661
CVE-2022-22597	CVE-2022-22628	CVE-2022-22662
CVE-2022-22598	CVE-2022-22629	CVE-2022-22664
CVE-2022-22599	CVE-2022-22631	CVE-2022-22665
CVE-2022-22600	CVE-2022-22632	CVE-2022-22666
CVE-2022-22601	CVE-2022-22633	CVE-2022-22667
CVE-2022-22602	CVE-2022-22634	CVE-2022-22668
CVE-2022-22603	CVE-2022-22635	CVE-2022-22669
CVE-2022-22604	CVE-2022-22636	CVE-2022-22670
CVE-2022-22605	CVE-2022-22637	CVE-2022-22671
CVE-2022-22606		

Fabricante

Apple

Productos afectados

macOS Catalina: 10.15 19A583 a 10.15.7 19H1715
macOS Monterey: 12.0 21A344 a 12.2.1 21D62
macOS Big Sur: 11.0 20A2411 a 11.6.4 20G417
Apple Xcode: 11.0 a 13.2.1
Apple GarageBand: 10.3 a 10.4.5
Apple Logic Pro X, versiones anteriores a la10.7.3
watchOS: 8.0 19R346 a 8.4.2 19S553

iTunes: 12.0 a 12.12.2 tvOS: 15.0 19J346 a 15.3 19K547 iPadOS: 15.0 19A346 a 15.3.1 19D52 Apple iOS: 15.0 19A346 a 15.3.1 19D52
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00594-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00594-01.pdf

CSIRT alerta de nueva vulnerabilidad en algunas versiones de OpenSSL	
Alerta de seguridad cibernética	9VSA22-00595-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2022
Última revisión	15 de marzo de 2022
CVE	
CVE-2022-0778	
Fabricante	
OpenSSL	
Productos afectados	
OpenSSL versiones 1.0.2, 1.1.1 y 3.0, que reciben parches. La versión 1.1.0 también es afectada, pero no será parchada. OpenSSL 1.0.2 deben actualizar a 1.0.2zd (exclusivo premium support) OpenSSL 1.1.1 deben actualizar a 1.1.1n OpenSSL 3.0 deben actualizar a 3.0.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00595-01/	
https://www.csirt.gob.cl/media/2022/03/9VSA22-00595-01.pdf	

CSIRT alerta de nuevas vulnerabilidades en el kernel de Linux	
Alerta de seguridad cibernética	9VSA22-00596-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de marzo de 2022
Última revisión	15 de marzo de 2022

CVE

CVE-2022-0847
CVE-2022-26966

Fabricante

Varios, que basan sus productos en el kernel de Linux

Productos afectados

Aquellos que usen Linux kernel en versiones anteriores a 5.16.12.

Algunos de los más populares son:
Red Hat
Red Hat Virtualization 4 for Red Hat Enterprise Linux 8
Red Hat Enterprise Linux 8
Red Hat Enterprise Linux 8.2 Extended Update Support
Red Hat Enterprise Linux 8.4 Extended Update Support
Red Hat Enterprise Linux 8
Red Hat Enterprise Linux 8.1 Update Services for SAP Solutions
Red Hat Enterprise Linux 8.2 Extended Update Support
Red Hat ya anunció parches para todos estos productos afectados

QNAP NAS: QTS 5.0.x y QuTS hero h5.0.x

SUSE
SUSE Linux Enterprise Micro 5.1
En proceso de parche
SUSE Linux Enterprise Server for SAP Applications 12 SP5
SUSE Linux Enterprise Server for SAP Applications 12 SP5
Parchados
SUSE Linux Enterprise Desktop 15 SP4
SUSE Linux Enterprise Desktop 15 SP4
SUSE Linux Enterprise High Performance Computing 15 SP4
SUSE Linux Enterprise High Performance Computing 15 SP4
SUSE Linux Enterprise High Performance Computing 15 SP4
SUSE Linux Enterprise Module for Basesystem 15 SP4
SUSE Linux Enterprise Module for Basesystem 15 SP4
SUSE Linux Enterprise Module for Development Tools 15 SP4
SUSE Linux Enterprise Module for Development Tools 15 SP4
SUSE Linux Enterprise Module for Public Cloud 15 SP4

SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 Debian 5.10.84-1
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00596-01/
https://www.csirt.gob.cl/media/2022/03/9VSA22-00596-01.pdf

Actualidad

Ciberconsejos para lograr comunidades educativas más seguras

Este 14 de marzo, como parte del Día Contra el Ciberacoso, el CSIRT de Gobierno junto con la Fundación Katy Summer se unieron para concientizar y educar a los padres y menores sobre cómo protegerse y apoyar a las víctimas del cyberbullying. Los ciberconsejos de esta semana los pueden descargar y compartir en formato PDF y como imágenes en formato PNG también aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-protegerse-del-ciberacoso/.

https://www.csirt.gob.cl
+ (562) 2486 3850
@csirtgob
@CSIRTConciencia
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.

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

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 (csirt.gob.cl o al 1510) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Camilla Agnese Giulietti Escudero
- Juan Pablo Berríos Isaacs
- Camilo Ignacio Ortúzar Aránguiz
- Juan Manuel Sanhueza Gómez
- Luis Eduardo Atala González
- Ashly Yihad Sepúlveda Vera
- Javier Ignacio Candia Tapia
- Christian Campodónico
- Andrés Peñailillo
- Jaime Contardo
- Victor Cofré
- Carlos de la Fuente Castro