Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

22-10-2021 | Año 3 | N°120

Boletín de Seguridad Cibernética

Semana del 15 al 21 de octubre de 2021

La semana en cifras

Hash

14

SHA

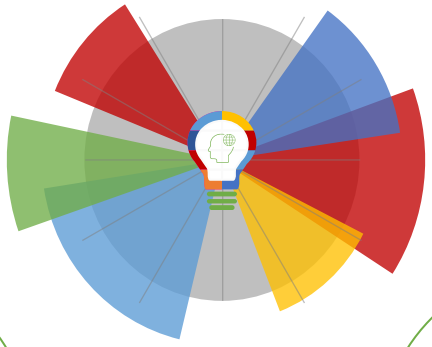
Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

4

URL

Asociadas a sitios fraudulentos y campañas de phishing



Parches

250

para vulnerabilidades

Las mitigaciones son útiles en productos de Google, Oracle y Cisco.

IP

1

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

Malware

CSIRT alerta de campaña de phishing que difunde malware a través de falsa factura	
Alerta de seguridad cibernética	2CMV21-00234-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2021
Última revisión	14 de octubre de 2021
Indicadores de compromiso	
SHA256	
A8FD3B40DFDD6ADD285CAA0670B678A6FC7C65CBF1BA487FED174789CCB7793 90BE634820B42505DA42769E83EBC62AB133090C810B64140C551FC4136C5FE7 0605BA2116585EB673DEA3125F0E48DCF90AC52A3E8725DF986EDDFF467A2B47	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00234-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00234-01.pdf	

CSIRT alerta de campaña de phishing que difunde malware a través de falsa factura	
Alerta de seguridad cibernética	2CMV21-00235-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2021
Última revisión	12 de octubre de 2021
Indicadores de compromiso	
SHA256	
67D1BFF9AE5FCD660ACC117C1D4F8F23DE4B6C43163B43514D08958FC31A241E F56AEBD741C745C86FC0B6BAB9E6BD537E9576DB187A78660D48C817089F5EE8	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00235-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00235-01.pdf	

Imagen del Mensaje

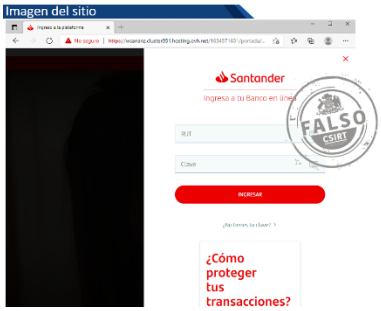
CSIRT alerta de campaña de phishing que difunde malware a través de falsa factura	
Alerta de seguridad cibernética	2CMV21-00236-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2021
Última revisión	19 de octubre de 2021
Indicadores de compromiso	
SHA256	
C507267271A4FD79A9AADF7732842F06C716A6836C48418AB6CAC8B2DF882E33 90BB4ACF70C8626F3CE6A9630437883BBFC62AE8AD344B673A8F005CE9D2AC30	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00236-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00236-01.pdf	

Imagen del Mensaje

CSIRT alerta de phishing con malware con supuesto comprobante de pago	
Alerta de seguridad cibernética	2CMV21-00237-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2021
Última revisión	19 de octubre de 2021
Indicadores de compromiso	
SHA256	
468C6FCC488DEE40E26EB222747F36854FBE9E58FA138CDF9B923FC2355B7CA8 90BB4ACF70C8626F3CE6A9630437883BBFC62AE8AD344B673A8F005CE9D2AC30 802C858F8EAE004082DA8F3F25B53DA7B0401F46912AD00E6E14DC6FF8E606A5 0BD094D1EE19A3B2B9B17CF89BF11D5A440C28215B9BF5665CD8AF353285EDFC	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00237-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00237-01.pdf	

CSIRT informa phishing con malware a través de una supuesta cotización	
Alerta de seguridad cibernética	2CMV21-00238-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2021
Última revisión	19 de octubre de 2021
Indicadores de compromiso	
SHA256	
38E1C5A41DDCC6B3571BE6368F397F6A3B450E2DE30D18189E7D35C0A4A39050 E5EBC473E259EC57E2A831477B449DD07C13198C0DB74CE67732A8FCE59E25AC 23E80D01CF007B17F91366FB1866568F0385FF08767434728F209535D3452FDD 7008543C4A44B254EBB0B84F36B96D62866C3B57AD698F3765CA7D5E77831600	
IoC Red	
https://www.theonionrouter[.]com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip http://www.zhhwl[.]com/ http://v.juhe[.]cn/sms/send http://api.weimi[.]cc/2/account/balance.html	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2CMV21-00238-01/	
https://csirt.gob.cl/media/2021/10/2CMV21-00238-01.pdf	

Sitios fraudulentos



CSIRT alerta sitio web que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR21-01014-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2021
Última revisión	18 de octubre de 2021
Indicadores de compromiso	
URL sitio falso	
http://wsananz.cluster051.hosting.ovh[.]net/1634571089/portada/personas/home.asp	
IP	
[51.161.122.78]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-01014-01/	
https://www.csirt.gob.cl/media/2021/10/8FFR21-01014-01.pdf	

Vulnerabilidades

CSIRT advierte de vulnerabilidades en Google Chrome	
Alerta de seguridad cibernética	9VSA21-00507-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de octubre de 2021
Última revisión	15 de octubre de 2021
CVE	
CVE-2021-37977	CVE-2021-37979
CVE-2021-37978	CVE-2021-37980
Fabricante	
Google	
Productos afectados	
Google Chrome: 7.0.517.41 a 94.0.4606.71.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00507-01	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00507-01.pdf	

CSIRT comparte vulnerabilidades informadas en varios productos de Oracle			
Alerta de seguridad cibernética	9VSA21-00508-01		
Clase de alerta	Vulnerabilidad		
Tipo de incidente	Sistema y/o Software Abierto		
Nivel de riesgo	Crítico		
TLP	Blanco		
Fecha de lanzamiento original	20 de octubre de 2021		
Última revisión	20 de octubre de 2021		
CVE			
CVE-2016-1000031	CVE-2021-22118	CVE-2021-35543	CVE-2021-35610
CVE-2016-2183	CVE-2021-22696	CVE-2021-35545	CVE-2021-35611
CVE-2017-9841	CVE-2021-22884	CVE-2021-35546	CVE-2021-35612
CVE-2018-10237	CVE-2021-22926	CVE-2021-35549	CVE-2021-35613
CVE-2018-20034	CVE-2021-22931	CVE-2021-35550	CVE-2021-35616
CVE-2018-20843	CVE-2021-23017	CVE-2021-35551	CVE-2021-35617
CVE-2018-8088	CVE-2021-2332	CVE-2021-35552	CVE-2021-35618
CVE-2019-0227	CVE-2021-23337	CVE-2021-35553	CVE-2021-35619
CVE-2019-10086	CVE-2021-2351	CVE-2021-35554	CVE-2021-35620
CVE-2019-11358	CVE-2021-23841	CVE-2021-35556	CVE-2021-35621
CVE-2019-12400	CVE-2021-23926	CVE-2021-35557	CVE-2021-35622
CVE-2019-12415	CVE-2021-2416	CVE-2021-35558	CVE-2021-35623
CVE-2019-13990	CVE-2021-2461	CVE-2021-35559	CVE-2021-35624
CVE-2019-17195	CVE-2021-2471	CVE-2021-35560	CVE-2021-35625
CVE-2019-3740	CVE-2021-2474	CVE-2021-35561	CVE-2021-35626
CVE-2019-7317	CVE-2021-2475	CVE-2021-35562	CVE-2021-35627
CVE-2020-10543	CVE-2021-2476	CVE-2021-35563	CVE-2021-35628
CVE-2020-10683	CVE-2021-2477	CVE-2021-35564	CVE-2021-35629
	CVE-2021-2478	CVE-2021-35565	CVE-2021-35630

CVE-2020-10878	CVE-2021-2479	CVE-2021-35566	CVE-2021-35631
CVE-2020-11022	CVE-2021-2480	CVE-2021-35567	CVE-2021-35632
CVE-2020-11023	CVE-2021-2481	CVE-2021-35568	CVE-2021-35633
CVE-2020-11987	CVE-2021-2482	CVE-2021-35569	CVE-2021-35634
CVE-2020-11988	CVE-2021-2483	CVE-2021-35570	CVE-2021-35635
CVE-2020-11994	CVE-2021-2484	CVE-2021-35571	CVE-2021-35636
CVE-2020-11998	CVE-2021-2485	CVE-2021-35572	CVE-2021-35637
CVE-2020-13956	CVE-2021-25122	CVE-2021-35573	CVE-2021-35638
CVE-2020-15824	CVE-2021-25215	CVE-2021-35574	CVE-2021-35639
CVE-2020-17521	CVE-2021-26272	CVE-2021-35575	CVE-2021-35640
CVE-2020-17530	CVE-2021-26691	CVE-2021-35576	CVE-2021-35641
CVE-2020-1945	CVE-2021-27290	CVE-2021-35577	CVE-2021-35642
CVE-2020-1967	CVE-2021-27807	CVE-2021-35578	CVE-2021-35643
CVE-2020-1968	CVE-2021-27906	CVE-2021-35580	CVE-2021-35644
CVE-2020-1971	CVE-2021-28165	CVE-2021-35581	CVE-2021-35645
CVE-2020-24750	CVE-2021-28363	CVE-2021-35582	CVE-2021-35646
CVE-2020-25648	CVE-2021-28657	CVE-2021-35583	CVE-2021-35647
CVE-2020-25649	CVE-2021-29425	CVE-2021-35584	CVE-2021-35648
CVE-2020-27216	CVE-2021-29505	CVE-2021-35585	CVE-2021-35649
CVE-2020-27218	CVE-2021-29921	CVE-2021-35586	CVE-2021-35650
CVE-2020-27824	CVE-2021-30468	CVE-2021-35588	CVE-2021-35651
CVE-2020-28052	CVE-2021-30640	CVE-2021-35589	CVE-2021-35652
CVE-2020-29661	CVE-2021-3156	CVE-2021-35590	CVE-2021-35653
CVE-2020-36189	CVE-2021-3177	CVE-2021-35591	CVE-2021-35654
CVE-2020-5258	CVE-2021-31812	CVE-2021-35592	CVE-2021-35655
CVE-2020-5398	CVE-2021-33037	CVE-2021-35593	CVE-2021-35656
CVE-2020-5413	CVE-2021-33560	CVE-2021-35594	CVE-2021-35657
CVE-2020-6950	CVE-2021-3450	CVE-2021-35595	CVE-2021-35658
CVE-2020-7226	CVE-2021-34558	CVE-2021-35596	CVE-2021-35659
CVE-2020-8203	CVE-2021-35043	CVE-2021-35597	CVE-2021-35660
CVE-2020-8622	CVE-2021-3517	CVE-2021-35598	CVE-2021-35661
CVE-2020-8908	CVE-2021-3518	CVE-2021-35599	CVE-2021-35662
CVE-2020-9484	CVE-2021-3522	CVE-2021-35601	CVE-2021-35665
CVE-2020-9488	CVE-2021-35536	CVE-2021-35602	CVE-2021-35666
CVE-2021-20227	CVE-2021-35537	CVE-2021-35603	CVE-2021-36090
CVE-2021-21345	CVE-2021-35538	CVE-2021-35604	CVE-2021-36222
CVE-2021-2137	CVE-2021-35539	CVE-2021-35606	CVE-2021-36374
CVE-2021-21409	CVE-2021-35540	CVE-2021-35607	CVE-2021-3711
CVE-2021-21702	CVE-2021-35541	CVE-2021-35608	CVE-2021-3712
CVE-2021-21783	CVE-2021-35542	CVE-2021-35609	CVE-2021-37695
CVE-2021-22112			

Fabricante

Oracle

Productos afectados

Oracle Essbase	Oracle Fusion Middleware
Oracle Global Lifecycle Management	Oracle Health Sciences Applications
Oracle GoldenGate	Oracle Hospitality Applications
Oracle Graph Server and Client	Oracle Hyperion
Oracle NoSQL Database	Oracle Insurance Applications
Oracle REST Data Services	Oracle Java SE
Oracle Secure Backup	Oracle JD Edwards

Oracle Spatial Studio Oracle SQL Developer Oracle Commerce Oracle Communications Applications Oracle Communications Oracle Construction and Engineering Oracle E-Business Suite Oracle Enterprise Manager Oracle Financial Services Applications	Oracle MySQL Oracle PeopleSoft Oracle Retail Applications Oracle Siebel CRM Oracle Supply Chain Oracle Systems Oracle Utilities Applications Oracle Virtualization
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00508-01	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00508-01.pdf	

CSIRT alerta de vulnerabilidades en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00509-01
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 2021
Última revisión	21 de octubre de 2021
CVE	
CVE-2021-1529 CVE-2021-34737 CVE-2021-34743 CVE-2021-34760 CVE-2021-34789	CVE-2021-34738 CVE-2021-40121 CVE-2021-40123 CVE-2021-34736 CVE-2021-40122
Fabricante	
Cisco	
Productos afectados	
Cisco IOS XE SD-WAN Cisco IOS XE Software Cisco Webex Software Cisco IOS XR Software 6.7.2 y posteriores, 7.1.2 y posteriores, y 7.2.1 y posteriores pero anteriores al 7.3.2 Cisco TMS Software Cisco Tetration Cisco ISE Software UCS C-Series Rack Servers in standalone mode UCS S-Series Storage Servers in standalone mode Cisco Meeting Server	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9VSA21-00509-01	
https://www.csirt.gob.cl/media/2021/10/9VSA21-00509-01.pdf	

Actualidad

Consejos para pymes protagonizaron esta semana la campaña del CSIRT de Gobierno y CSIRTAmericas por el Mes de la Ciberseguridad

Octubre es el Mes de la Ciberseguridad y por eso 12 CSIRT del continente — reunidos en CSIRTAmericas— y el Programa de Ciberseguridad de la Organización de los Estados Americanos (OEA) hemos compartido una serie de ciberconsejos de concientización alineados según cuatro temas, uno cada semana.

Esta tercera semana nuestros ciberconsejos fueron dirigidos a pequeñas y medianas empresas, entregando recomendaciones para mantener sus redes y a sus empleados más seguros. El turno fue de los CSIRT de Panamá, Estados Unidos y Jamaica.

La idea, presentada por el CSIRT del Gobierno de Chile a CSIRTAmericas y adoptada rápidamente, ha sido plasmada en imágenes en nuestro país recopilando consejos enviados por cada uno de los CSIRT partícipes: Buenos Aires y Neuquén en Argentina, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Jamaica, Panamá, Paraguay, República Dominicana y Uruguay. Las publicaciones son hechas en inglés y castellano y podrán verlas aparecer durante todo el mes en https://twitter.com/CSIRTGOB.


Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
PYMES
Cuando trabajas desde casa recuerda que el perímetro de seguridad de la oficina se extiende hasta tu ubicación física:
NUNCA te conectes a la red de tu empresa sin utilizar una VPN. Siempre utiliza los medios más seguros para conectarte a las redes corporativas.
CSIRTAmericas Network


Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
PYMES
Para fortalecer la ciberseguridad en tu empresa, recuerda los siguientes consejos:
REALIZA y VERIFICA tus copias de seguridad de forma periódica.
MANTEN actualizados tus activos informáticos recurrentemente.
FOMENTA una cultura de ciberseguridad en tu organización.
CSIRTAmericas Network


Ciberconsejos para el
MES DE LA CIBERSEGURIDAD
PYMES
PROMUEVE que los empleados utilicen contraseñas complejas y únicas para los diferentes sitios que visitan. Los gestores de contraseñas ayudan a recordar esas contraseñas complicadas.
CSIRTAmericas Network

El Comando de la Semana | No. 22 Lynis

El protagonista en una nueva edición de El Comando de la Semana es Lynis, una herramienta de auditoría de seguridad, de código abierto. Su principal objetivo es auditar y fortalecer los sistemas basados en Unix y Linux, todo esto para facilitar el hardening o «endurecimiento» de nuestros sistemas, proceso en el cual reforzamos su seguridad por medio de la eliminación de vulnerabilidades y puntos débiles de nuestros sistemas, purgando software, servicios, cuentas de usuario o puertos, entre otros, que ya no estemos utilizando.

Con los comandos que compartimos semanalmente no pretendemos reemplazar una auditoria de código o evaluación de vulnerabilidades, sino que establecer capacidades básicas de chequeo y obtención de información de manera rápida para temas específicos, como por ejemplo la verificación de la subsanación de alertas o vulnerabilidades reportadas por el CSIRT de Gobierno.

Encuentra el comando de esta semana aquí: https://www.csirt.gob.cl/estadisticas/el-comando-de-la-semana-no-22.

El Control de la Semana | No. 16 Gestión de las vulnerabilidades técnicas

La Ficha de Control Normativo de esta semana trata sobre los procedimientos para la Gestión de las vulnerabilidades técnicas, con recomendaciones y mejores prácticas relativas a su control.

Se debe obtener información acerca de las vulnerabilidades técnicas de los sistemas de información usados, y hacerlo de manera oportuna. Asimismo, es necesario evaluar la exposición de la organización a estas vulnerabilidades y tomar medidas apropiadas para abordar el riesgo asociado. Además, se deben construir políticas y procedimientos que ayuden a establecer las directrices de ciberseguridad y guías operacionales que permitan a todos los intervinientes implementar y utilizar los software operacionales de manera segura. El CSIRT de Gobierno ha preparado algunas políticas que pueden servir de punto de partida para aquellas

En el documento descargable a continuación encontrarán todos los detalles del control de esta semana: https://www.csirt.gob.cl/estadisticas/el-control-de-la-semana-no-16

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 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.

- Pedro Arnaldo Rodríguez Brito
- Juan Correo
- Fernando Flores Tobar
- Eduardo Riveros Roca
- Carlos Barríos
- Victor Cofre
- Cat.py_01
- Erwin
- Joseph De Freitas
- Patricio Pérez Cárcamo
- José Ignacio Parra
- José Ignacio Ávila Silva
- Elisa Molina H.
- Victor Cofré
- Juan José Arriagada

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.10.22 16:14:39 -03'00'