CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

26-01-2020 | Año 2 | N°73

Boletín de Seguridad Cibernética

Semana del 19 al 25 de Noviembre de 2020

División de Redes y Seguridad Informática. Gobierno de Chile

Ministerio del Interior y Seguridad Pública. Gobierno de Chile

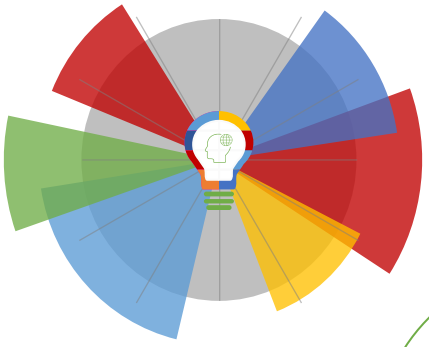
Resumen de la semana en cifras

Se advirtieron

4

URLs

Asociadas a sitios fraudulentos y campañas de phishing



Parches

56

para vulnerabilidades

Las mitigaciones son útiles para productos Mozilla, VMware, Google, NodeJS y Drupal.

IPs

91

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

Contenido

Sitios fraudulentos

CSIRT informa de página bancaria falsa	
Alerta de seguridad cibernética	8FFR20-00834-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Noviembre de 2020
Última revisión	19 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//creditoalinstantebancoestado[.]cl/mispersonales/imagenes/comun2008/banca-en-linea-personas.html	
IP	
186.64.118.235	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00834-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00834-01.pdf	

CSIRT advierte sobre sitio que suplanta servicio de streaming	
Alerta de seguridad cibernética	8FFR20-00835-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de Noviembre de 2020
Última revisión	21 de Noviembre de 2020
Indicadores de compromiso	
URL	
https[:]//puntaarenas[.]cl/.Logs/net/	
IP	
200[.]91[.]27[.]21	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr20-00835-01/	
https://www.csirt.gob.cl/media/2020/11/8FFR20-00835-01.pdf	

Phishing

CSIRT advierte de phishing bancario por error de cuenta	
Alerta de seguridad cibernética	8FPH20-00329-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2020
Última revisión	23 de Noviembre de 2020
Indicadores de compromiso	
URL	
http[:]//compuxchange.com/wp-content/cache/enviar03[.]php?l=139057626	
http[:]//www-bancoestado-cl.earlgreenwellness.co[.]uk/	
IP	
162.144.82.120	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph20-00329-01/	
https://www.csirt.gob.cl/media/2020/11/8FPH20-00329-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades que afectan a Mozilla Firefox	
Alerta de seguridad cibernética	9VSA20-00323-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de Noviembre de 2020
Última revisión	19 de Noviembre de 2020
CVE	
CVE-2020-26951 - CVE-2020-26952 - CVE-2020-16012 CVE-2020-26953 - CVE-2020-26954 - CVE-2020-26955 CVE-2020-26956 - CVE-2020-26957 - CVE-2020-26958 CVE-2020-26959 - CVE-2020-26960 - CVE-2020-15999 CVE-2020-26961 - CVE-2020-26962 - CVE-2020-26963 CVE-2020-26964 - CVE-2020-26965 - CVE-2020-26966 CVE-2020-26967 - CVE-2020-26968 - CVE-2020-26969	
Fabricante	
Mozilla	
Productos afectados	
La vulnerabilidad afecta al explorador web Firefox Mozilla versiones anteriores a la 83. La vulnerabilidad afecta al explorador web Firefox Mozilla ESR versiones anteriores a la 78.5. La vulnerabilidad afecta al cliente de correo Mozilla Thunderbird versiones	

anteriores a la 78.5.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00323-01/
https://www.csirt.gob.cl/media/2020/11/9VSA20-00323-01-2.pdf

CSIRT comparte actualizaciones obtenidas de VMware	
Alerta de seguridad cibernética	9VSA20-00324-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2020
Última revisión	23 de Noviembre de 2020
CVE	
CVE-2020-3997 - CVE-2020-3998 - CVE-2020-3984 CVE-2020-3985 - CVE-2020-4000 - CVE-2020-4001 CVE-2020-4002 - CVE-2020-4003 - CVE-2020-4004 CVE-2020-4005	
Fabricante	
VMware	
Productos afectados	
Horizon Server versión 7.x para cualquier sistema operativo. Horizon Client versión 5.x y anteriores para el sistema operativo Windows. SD-WAN Orchestrator versión 3.x. SD-WAN Orchestrator versiones 4.x y 3.x para Linux. VMware ESXi versiones 7.0, 6.7 y 6.5. VMware Cloud Foundation versiones 4.x y 3.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00324-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00324-01-1.pdf	

CSIRT comparte actualizaciones de Google para Chrome	
Alerta de seguridad cibernética	9VSA20-00325-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2020
Última revisión	23 de Noviembre de 2020
CVE	
CVE-2020-16018 - CVE-2020-16019 - CVE-2020-16020 CVE-2020-16021 - CVE-2020-16022 - CVE-2020-16015 CVE-2020-16014 - CVE-2020-16023 - CVE-2020-16024 CVE-2020-16025 - CVE-2020-16026 - CVE-2020-16027 CVE-2020-16028 - CVE-2020-16029 - CVE-2020-16030 CVE-2019-8075 - CVE-2020-16031 - CVE-2020-16032 CVE-2020-16033 - CVE-2020-16034 - CVE-2020-16035 CVE-2020-16012 - CVE-2020-16036	
Fabricante	
Google	
Productos afectados	
Google Chrome versiones anteriores a la 87.0.4280.66 en Windows y Linux, y 87.0.4280.67 en Mac.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00325-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00325-01.pdf	

CSIRT comparte mitigación para vulnerabilidad obtenida de NodeJS	
Alerta de seguridad cibernética	9VSA20-00326-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de Noviembre de 2020
Última revisión	23 de Noviembre de 2020
CVE	
CVE-2020-8277	
Fabricante	
NodeJS	
Productos afectados	
Versiones 12.16.3 y superiores en la línea 12.x. Versiones 14.13.0 y superiores en la línea 14.x Todas las versiones de la línea 15.x.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00326-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00326-01.pdf	

CSIRT comparte mitigación para vulnerabilidad en Drupal	
Alerta de seguridad cibernética	9VSA20-00327-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Noviembre de 2020
Última revisión	24 de Noviembre de 2020
CVE	
CVE-2020-13671	
Fabricante	
Drupal	
Productos afectados	
Drupal versiones 9.x, 8.9.x, 8.8.x y anteriores y 7.x y anteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa20-00327-01/	
https://www.csirt.gob.cl/media/2020/11/9VSA20-00327-01.pdf	

IoC - Ataques e 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) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	
5.196.217.176	141.98.80.80
14.186.196.217	155.12.21.118
14.226.246.151	158.69.157.46
37.221.178.100	170.233.69.109
37.221.179.151	170.250.245.40
37.221.179.187	178.156.67.180
37.221.182.229	186.179.100.10
37.221.183.192	186.68.86.234
60.211.217.154	187.25.227.218
76.184.134.253	188.255.131.70
88.148.113.227	189.114.93.191
109.166.168.111	191.102.83.167
111.202.130.168	194.208.93.9
121.160.165.136	195.32.73.160
178.254.171.149	195.32.73.73
178.254.171.178	197.248.20.2
178.254.179.153	198.27.110.178
178.254.179.198	200.91.55.236
178.254.179.250	212.69.22.168
186.179.100.115	212.69.22.190
186.179.100.203	212.69.22.20
186.239.134.158	212.69.24.226
188.255.131.183	212.69.27.222
188.255.131.245	218.22.180.146
188.255.132.165	218.85.143.78
188.255.132.181	221.13.140.88
188.255.132.221	23.240.136.91
188.255.132.239	31.170.59.35
188.255.237.161	37.221.181.3

188.255.237.188	37.221.181.51
188.255.237.208	37.221.181.69
191.102.120.181	37.221.182.8
102.68.7.160	37.99.254.197
103.89.89.210	41.202.170.77
104.136.140.15	41.86.238.176
120.33.137.113	45.165.214.24
121.133.34.48	5.196.201.7
123.24.186.225	60.29.37.54
124.88.218.106	60.30.162.38
128.92.1.162	62.20.175.84
14.177.18.134	74.51.2.240
14.179.15.195	80.210.22.96
14.186.48.196	85.105.206.68
141.105.104.43	95.38.101.206

Actualidad

Ciberguía para la violencia contra la mujer

Durante muchos años las mujeres han sido víctimas de violencia, incluso desde la etapa escolar donde el bullying es uno de los principales problemas, afectando principalmente a las niñas. Lamentablemente, este tipo de agresión ya no se vive solamente en el colegio, sino que también está presente en el mundo virtual, por lo que el impacto emocional en la vida de las personas puede ser aún mayor. El 25 de noviembre se conmemora el "Día Internacional de la Eliminación de la Violencia contra la Mujer", es por ello que queremos entregarte recomendaciones y los contenidos necesarios para apoyar la prevención.








Ver más: https://www.csirt.gob.cl/recomendaciones/ciberguia-para-la-vilencia-contra-la-mujer/

Investigación

Ransomware: del acceso inicial al compromiso de la red

La versión 22 de Análisis de Amenazas Cibernéticas fue elaborada por el investigador Germán Fernández, Líder Red Team y Threat Intelligence en CronUp, quien aborda el ransomware enfocándose en el ciclo de vida de la amenaza. El autor explica que el ransomware es una amenaza que está generando billones de dólares de ganancias para quienes perpetran estos ataques, a costa de miles de víctimas que pierden dinero, ven paraliza sus operaciones y recientemente, incluso ha costado la vida de una persona.

La comprensión del ciclo de vida del ransomware, conocido como el cyber kill chain, es clave para entender detectar, detener e interrumpir, así como para crear las protecciones esenciales frente a la amenaza. Este artículo fue organizado en cuatro secciones de investigación y aborda los principales vectores de ataques cuando ocurre un ransomware, los que explica en detalles en el punto 3 de este trabajo, como el phishing y la ingeniería social, los RDP expuestos a internet, las vulnerabilidades de software, los troyanos bancarios, el malversiting y los kits de herramientas utilizadas. En la sección cuatro, el autor comparte un interesante gráfico que muestra las víctimas de los ransomware en el último tiempo, y finaliza el artículo dando una serie de recomendaciones para hacer frente a la amenaza.

Ver más: https://www.csirt.gob.cl/reportes/an2-2020-21-2/

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 Ignacio Ávila
- Martín Estay
- Claudio Valderrama
- Gloria Ugarte
- Rodrigo Machado

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.11.27 12:54:57 -03'00'