CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 226

semana del 26 de octubre al 2 de noviembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

1

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

2

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

47

Las mitigaciones son útiles en productos de F5, Cisco, Atlassian y Google.

CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Phishing

Imagen 1: Correo Electrónico

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00903-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 octubre, 2023
Última revisión	31 octubre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://undercodesmstado[.]com/1698758461/imagenes/_personas/home/default.asp	
URL de redirección	
https://patitojouxstore[.]com/activacion/cuenta-efqc/	
Dirección IP sitio falso	
[198.27.78.113]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00903-01/	

2. Vulnerabilidades

CSIRT informa de vulnerabilidades en NGINX Ingress para Kubernetes	
Alerta de seguridad cibernética	9VSA23-00926-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 octubre, 2023
Última revisión	30 octubre, 2023
CVE	
CVE-2022-4886 CVE-2023-5043 CVE-2023-5044	
Fabricante	
F5	
Productos afectados	
NGINX Ingress Controller	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00926-01/	

CSIRT informa de vulnerabilidad crítica que afecta a BIG-IP	
Alerta de seguridad cibernética	9VSA23-00927-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 octubre, 2023
Última revisión	30 octubre, 2023
CVE	
CVE-2023-46747	
Fabricante	
F5	
Productos afectados	
BIG-IP 17.1.0 (Fixed in 17.1.0.3 + Hotfix-BIGIP-17.1.0.3.0.75.4-ENG) BIG-IP 16.1.0 – 16.1.4 (Fixed in 16.1.4.1 + Hotfix-BIGIP-16.1.4.1.0.50.5-ENG) BIG-IP 15.1.0 – 15.1.10 (Fixed in 15.1.10.2 + Hotfix-BIGIP-15.1.10.2.0.44.2-ENG) BIG-IP 14.1.0 – 14.1.5 (Fixed in 14.1.5.6 + Hotfix-BIGIP-14.1.5.6.0.10.6-ENG) BIG-IP 13.1.0 – 13.1.5 (Fixed in 13.1.5.1 + Hotfix-BIGIP-13.1.5.1.0.20.2-ENG).	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00927-01/	

CSIRT de Gobierno comparte información de nuevas vulnerabilidades críticas en Cisco IOS XE Software Web UI Feature	
Alerta de seguridad cibernética	9VSA23-00928-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 octubre, 2023
Última revisión	30 octubre, 2023
CVE	
CVE-2023-20198 CVE-2023-20273	
Fabricante	
Cisco	
Productos afectados	
Cisco IOS XE Software, si la función UI está activada	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00928-01/	

CSIRT comparte información de nueva vulnerabilidad crítica en Atlassian Confluence Data Center and Server	
Alerta de seguridad cibernética	9VSA23-00929-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 octubre, 2023
Última revisión	31 octubre, 2023
CVE	
CVE-2023-22518	
Fabricante	
Atlassian	
Productos afectados	
Todas las versiones de Atlassian Confluence Data Center and Server	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00929-01/	

CSIRT informa de nuevas vulnerabilidades parchadas en Google Chrome 119	
Alerta de seguridad cibernética	9VSA23-00930-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 noviembre, 2023
Última revisión	2 noviembre, 2023

CVE

CVE-2023-5480	CVE-2023-5852	CVE-2023-5856
CVE-2023-5482	CVE-2023-5853	CVE-2023-5857
CVE-2023-5849	CVE-2023-5854	CVE-2023-5858
CVE-2023-5850	CVE-2023-5855	CVE-2023-5859
CVE-2023-5851		

Fabricante

Google

Productos afectados

Google Chrome

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00930-01/

CSIRT comparte información de varias vulnerabilidades parchadas por Cisco en su Cisco ASA, FMC, and FTD Software Security Advisory Bundled Publication	
Alerta de seguridad cibernética	9VSA23-00931-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 noviembre, 2023
Última revisión	2 noviembre, 2023

CVE

CVE-2023-20048	CVE-2023-20042	CVE-2023-20270
CVE-2023-20086	CVE-2023-20114	CVE-2023-20246
CVE-2023-20095	CVE-2023-20264	CVE-2023-20071
CVE-2023-20244	CVE-2023-20005	CVE-2023-20247
CVE-2023-20083	CVE-2023-20041	CVE-2022-20713
CVE-2023-20063	CVE-2023-20074	CVE-2023-20070
CVE-2023-20155	CVE-2023-20206	CVE-2023-20267
CVE-2023-20219	CVE-2023-20245	CVE-2023-20031
CVE-2023-20220	CVE-2023-20256	CVE-2023-20177

Fabricante

Cisco

Productos afectados

Cisco ASA, FMC y FTD

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00931-01/

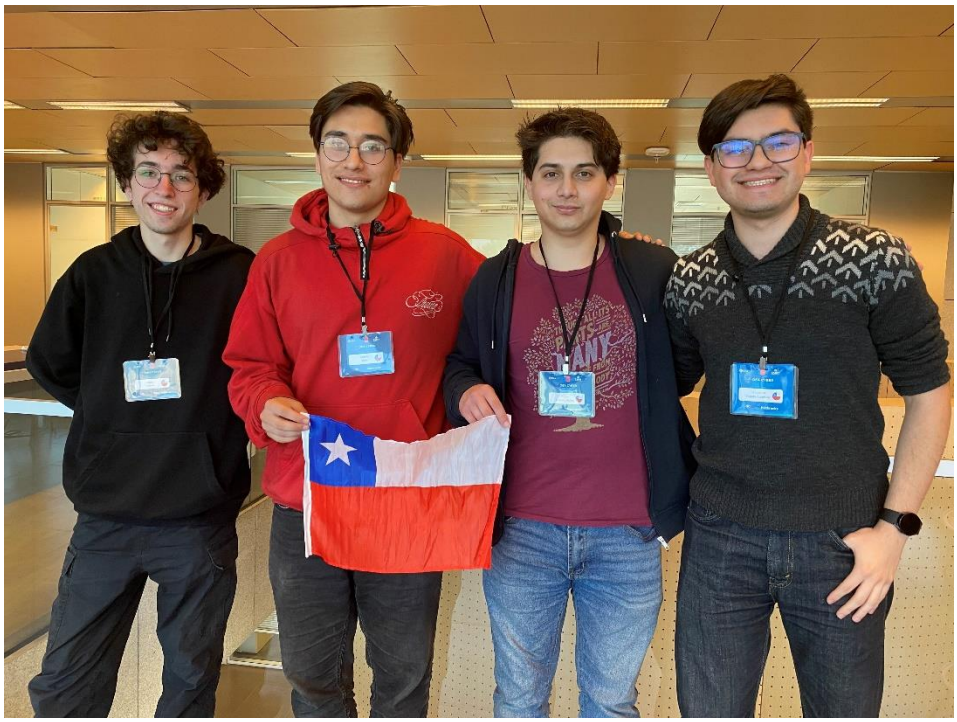
3. Noticias y concientización

Inteligencia de Amenazas: Ransomware BabLock

Nuestros expertos Kevin Anguita y César López, con el apoyo de Eduardo Riveros, prepararon este nuevo informe de Inteligencia de Amenazas, donde detallan lo que sabemos en el CSIRT sobre el ransomware que afectó a una compañía nacional durante octubre de 2023. Esperamos les resulte de utilidad.

El informe lo pueden descargar aquí: https://csirt.gob.cl/reportes/14tca23-00015-01/

Chile obtiene el primer lugar en el OEA Cyber Challenge



Entre el 25 y 26 de octubre se llevó a cabo por primera vez en Chile la final del OEA Cyber Challenge, una competencia de ciberseguridad para personas entre 18 y 30 años. Tras una intensa y disputada jornada, Chile obtuvo el primer lugar, logrando descifrar todos los desafíos en el menor tiempo posible. El segundo lugar lo obtuvo Perú, quien también resolvió todos los escenarios y Brasil ocupó el tercer lugar.

El equipo de los chilenos estuvo conformado por Diego Arias, Camilo Vera, Sebastián Zapata y Pablo Aravena, quienes mostraron un excelente resultado. Si bien no se conocían entre ellos, hicieron un gran trabajo en equipo. “El ejercicio nos pareció bastante interesante desde el punto de vista de los desafíos, fueron variados y bien entretenidos”, aseguraron los ganadores. Además, agregaron: “Uno siempre está constantemente practicando y resolviendo desafíos de todo tipo, por lo que todo sirve y suma, y jugamos con harta motivación. Los CTF permiten acercarse al mundo laboral de la ciberseguridad, ya que uno se enfrenta a desafíos parecidos a los que nos podemos encontrar en la realidad y la idea es explotar esa creatividad para encontrar vulnerabilidades”.

Asimismo, Cristian Bravo Lillo, director del CSIRT de Gobierno, aseguró: “La ciberseguridad es un área cada día con más relevancia en nuestro país y en el mundo, por lo tanto, debemos ocuparnos de esto y ser capaces de avanzar de forma integral, considerando todos los aspectos que involucra la seguridad de la información. Esto es, por ejemplo, fomentar el desarrollo de profesionales, incentivar la capacitación y el desarrollo de habilidades, promover el trabajo en equipo y cooperación entre los países. Y esta es una de las tantas aristas en la que estamos trabajando, lo que se refleja en este tipo de eventos”.

La nota completa: https://csirt.gob.cl/noticias/chile-primer-lugar-oea-cyber-challenge/

Subsecretaría del Interior organiza conversatorio «Ciberseguridad y Riesgos del Ciberacoso"

Un interesante conversatorio sobre ciberseguridad y riesgos del ciberacoso, organizó la Unidad de Género y Participación Ciudadana de la Subsecretaría del Interior con el apoyo del CSIRT de Gobierno el pasado 30 de octubre. La actividad contó con charlas del subprefecto Roberto Arriagada, jefe del Equipo de Investigación contra la Explotación Sexual de la Unidad Especializada del Cibercrimen de la PDI, y de Evanyely Zamorano y Emanuel Pacheco, quienes formaron la Fundación Katy Summer. Nuestro resumen sobre la jornada lo pueden encontrar aquí: https://csirt.gob.cl/noticias/conversatorio-ciberseguridad-y-ciberacoso/

Como parte de la apertura de la instancia, Cristian Bravo, director del CSIRT, se refirió a los incidentes cibernéticos que han afectado al sector público en el último tiempo: "A través de datos nos hemos dado cuenta de que lo que le gusta hablar a los técnicos (sistemas de seguridad perimetral) no es un factor importante. Lo relevante es la cantidad de problemas que tenemos hoy en día en Internet».

En este sentido, el director citó una investigación realizada por el gobierno del Reino Unido en 2007: «Llegaron a la conclusión de que existen tres tipos de delitos: el primero consiste de delitos tradicionales, que ya eran cometidos antes de que surgiera Internet y hoy se siguen perpetuando con una diferencia: el medio. El segundo son los llamados transicionales, que también se cometían antes de Internet, pero que en la actualidad se ven potenciados. En esta clasificación está el ciberacoso, la pornografía infantil y otra serie de fenómenos. El tercer tipo abarca delitos que se comenten solo desde que existe Internet, como el phishing".

Ciberconsejos | Cómo evitar estafas en personas mayores

Cerramos el Mes de la Ciberseguridad con recomendaciones para las personas mayores. De acuerdo con el estudio «Radiografía Digital en Personas Mayores» del año 2022, un tercio de las personas mayores encuestadas han sido víctima de estafas digitales, principalmente, con tarjetas y cuentas bancarias. Existen distintas técnicas para cometer las estafas, entre ellas, phishing, smishing y vishing, y en todos estos casos el delincuente busca obtener robar dinero u obtener información de la víctima suplantando la identidad de una institución o una persona.

La campaña completa, para descargar y compartir sus infografías con sus trabajadores, amigos y familiares, aquí: https://csirt.gob.cl/noticias/conversatorio-ciberseguridad-y-ciberacoso/

4. 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 que los sitios web a los que se ingrese sean los oficiales.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.03 14:26:24 -03'00'