CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 232

semana del 7 al 14 de diciembre de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

2

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

4

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

41

Las mitigaciones son útiles en productos de Google, Microsoft y Apple.

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	8FPH23-00913-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 diciembre, 2023
Última revisión	11 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://patitojouxstores[.]com/1701872777/imagenes/_personas/home/default.asp	
URL de redirección	
https://contrystadosuport[.]com/activacion/cuenta-funb/	
Dirección IP sitio falso	
[198.27.78.113]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00913-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00914-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 diciembre, 2023
Última revisión	11 diciembre, 2023
Indicadores de compromiso	
URL del sitio falso	
https://consumo60cuotashome[.]com/1702299489/imagenes/_personas/home/default.asp	
URL de redirección	
https://contrystadosuport[.]com/activacion/cuenta-funb/	
Dirección IP sitio falso	
[198.27.78.113]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00914-01/	

2. Vulnerabilidades

CSIRT comparte información de nuevas vulnerabilidades parchadas en Google Chrome 120	
Alerta de seguridad cibernética	9VSA23-00941-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 diciembre, 2023
Última revisión	7 diciembre, 2023
CVE	
CVE-2023-6508 CVE-2023-6509 CVE-2023-6510 CVE-2023-6511 CVE-2023-6512	
Fabricante	
Google	
Productos afectados	
Google Chrome, todas las versiones anteriores a la 120.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00941-01/	

CSIRT comparte información de vulnerabilidades parchadas por Apple para varios dispositivos	
Alerta de seguridad cibernética	9VSA23-00942-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 diciembre, 2023
Última revisión	12 diciembre, 2023
CVE	
CVE-2023-42916 CVE-2023-42917	
Fabricante	
Apple	
Productos afectados	
iPhone 8 y posteriores. iPad Pro, iPad Air tercera generación y posteriores, iPad quinta generación y posteriores y iPad mini quinta generación y posteriores. Apple TV HD y Apple TV 4K. Apple Watch serie 4 y posteriores.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00942-01/	

CSIRT comparte información de actualización de seguridad de Microsoft para diciembre 2023	
Alerta de seguridad cibernética	9VSA23-00943-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 diciembre, 2023
Última revisión	13 diciembre, 2023

CVE

CVE-2023-35621	CVE-2023-35643	CVE-2023-21740
CVE-2023-35622	CVE-2023-35642	CVE-2023-35644
CVE-2023-35619	CVE-2023-35641	CVE-2023-36012
CVE-2023-20588	CVE-2023-35639	CVE-2023-35634
CVE-2023-36696	CVE-2023-35638	CVE-2023-35625
CVE-2023-35635	CVE-2023-36006	CVE-2023-35624
CVE-2023-35633	CVE-2023-36005	CVE-2023-36019
CVE-2023-35632	CVE-2023-36004	CVE-2023-36020
CVE-2023-35631	CVE-2023-36003	CVE-2023-35636
CVE-2023-35630	CVE-2023-36011	CVE-2023-36010
CVE-2023-35629	CVE-2023-36009	CVE-2023-36391
CVE-2023-35628		

Fabricante

Microsoft

Productos afectados

Azure Connected Machine Agent
Azure Logic Apps
Azure Machine Learning SDK
Dynamics 365 for Finance and Operations Platform Update 60
Dynamics 365 for Finance and Operations Version 10.0.37 Platform Update 61
Dynamics 365 for Finance and Operations Version 10.0.38 Platform Update 62
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 9.1
Microsoft Malware Protection Platform
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Power Platform
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 22H2 for 32-bit Systems

	Windows 10 Version 22H2 for ARM64-based Systems Windows 10 Version 22H2 for x64-based Systems Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems Windows 11 Version 22H2 for ARM64-based Systems Windows 11 Version 22H2 for x64-based Systems Windows 11 Version 23H2 for ARM64-based Systems Windows 11 Version 23H2 for x64-based Systems Windows Server 2008 for 32-bit Systems Service Pack 2 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server 2022, 23H2 Edition (Server Core installation)
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00943-01/

3. Noticias y concientización

Congreso aprueba Ley Marco de Ciberseguridad, que fortalece institucionalidad y crea agencia nacional

Este martes, el Senado dio la última aprobación que necesitaba la Ley Marco de Ciberseguridad e Infraestructura Crítica para entrar en vigor, faltando únicamente su promulgación por parte del Presidente de la República y su consiguiente publicación en el Diario Oficial.

La iniciativa «fue votada tanto la Cámara de Diputados como el Senado de forma unánime», destacó la ministra del Interior, Carolina Tohá, quien agradeció ese alto respaldo y resaltó la importancia de la aprobación de la Ley Marco: «Este proyecto nos va a poner a la vanguardia en la región latinoamericana en esta materia. Vamos a tener una agencia encargada de la ciberseguridad, que va a definir estándares, tanto para los servicios esenciales como para los operadores que tienen funciones vitales, y esos estándares van a ser validados a través de instituciones certificadas especialmente para cumplir esa tarea».

La noticia completa en nuestro sitio web: https://csirt.gob.cl/noticias/congreso-aprueba-ley-marco/.

Crea la Agencia Nacional de Ciberseguridad (ANCI), que consolida administrativamente y dota de mayores recursos a la protección de la ciberseguridad en nuestro país, mejorando y ampliando el trabajo que hoy realiza el CSIRT de Gobierno para que ocurran menos incidentes digitales y para responder de mejor manera a los que pese a todo seguirán teniendo lugar.

La ANCI será un servicio público descentralizado, con patrimonio propio y carácter técnico y especializado, cuyo director será designado según las normas del Sistema de Alta Dirección Pública. Definirá protocolos y reglamentos de seguridad que las instituciones estarán obligadas a implementar, medidas que buscan que

estas mismas instituciones puedan prevenir y resolver incidentes de ciberseguridad, protegiendo así sus activos digitales, su información y la de los ciudadanos.
La ANCI también contará con facultades para fiscalizar y sancionar a las instituciones que no mejoren su ciberseguridad de acuerdo con dichos estándares, o no respondan adecuadamente a los incidentes que sucedan. Asimismo, colaborará y asesorará de manera técnica a otras instituciones afectadas por un incidente de ciberseguridad, siempre que sus recursos se lo permitan.

Junto con la ANCI, se crean también el CSIRT Nacional y el CSIRT de Defensa. Recordemos que un CSIRT es un equipo de especialistas dedicado a evitar que sucedan incidentes de ciberseguridad, y a solucionarlos cuando ocurren. El organismo encargado de coordinar a todos estos CSIRT será, precisamente, la ANCI.

Se hará hincapié en la seguridad de los servicios esenciales (SE), no importando si estos sean administrados por el Estado, empresas públicas o privadas. Entre ellos se encuentran actividades de generación eléctrica, distribución de combustible y transporte terrestre, aéreo, ferroviario y marítimo, servicios financieros y prestación institucional de salud.

También se protegerá mejor la seguridad de la infraestructura crítica de la información, los denominados Operadores de Importancia Vital (OIV). Para SE y OIV habrá multas si no cumplen con la debida protección de su ciberseguridad.

Asimismo, la ley considera obligaciones para las empresas privadas de ocuparse de los incidentes de ciberseguridad, y de informar cuanto antes a la ANCI de cualquier problema serio, junto con crear mejores instancias de coordinación público-privadas, todo lo que ayudará a combatir y solucionar incidentes de seguridad más rápidamente, reduciendo los efectos de estos incidentes para la ciudadanía.

La ley marco instaura así un modelo de gobernanza y mecanismos para contar siempre con los más actualizados estándares de seguridad, campañas de concientización para la ciudadanía, y los equipos necesarios para evitar y responder ante incidentes de ciberseguridad.

La noticia completa en nuestro sitio web: https://csirt.gob.cl/noticias/congreso-aprueba-ley-marco/.

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.

5. 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 campañas de phishing, malware y/o sitios fraudulentos.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono 1510), siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- Francisco Javier Gutiérrez Phishing
- Fabián Alexis Pereira Pereira Phishing
- Mauricio Díaz Mena Phishing
- Brady Gabriel Ramos Muñoz Redireccionamiento
- Bastián Enzo Armando Muñoz Villegas Phishing
- Roberto Nanjarí Phishing
- Francisco Gutiérrez Directorio Expuesto
- Marcelo Araneda Phishing
- Claudio Urquiza Rojas Phishing

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.12.20 11:33:46 -03'00'