Ministerio del Interior y Seguridad Pública

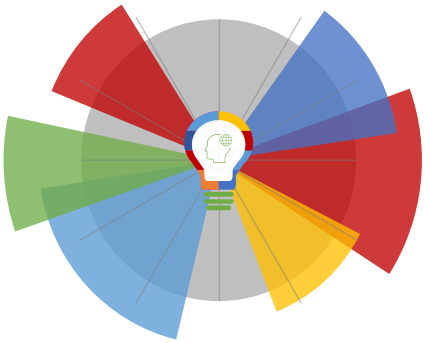
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

14-04-2022 | Año 4 | N°145

Boletín de Seguridad Cibernética

Semana del 8 al 13 de abril de 2022

La semana en cifras



Se advirtieron

7

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Parches

171

para vulnerabilidades

Sus mitigaciones son útiles en productos de Microsoft, Mozilla, Google, VMware y Adobe.

IP

4

Informadas

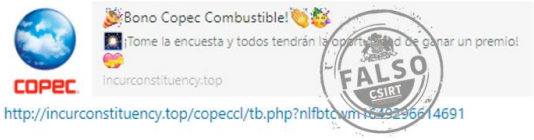
Listado de IP advertidas en múltiples campañas de phishing y de malware.

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

Contenido

Phishing

Imagen del mensaje



CSIRT advierte phishing con falso concurso de Copec	
Alerta de seguridad cibernética	8FPH22-00508-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2022
Última revisión	11 de abril de 2022
Indicadores de compromiso	
URL redirección	
http://incurconstituency[.]top/copeccl/tb.php?nlfbtcwm1649296614691	
URL sitio falso	
https://carddecide[.]top/b3xh2mQ4/copeccl/?_t=1649688868253#1649688871117	
IP	
[104.21.96.2]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00508-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00508-01.pdf	

Imagen del mensaje

CSIRT informa de phishing que suplanta al Banco Falabella	
Alerta de seguridad cibernética	8FPH22-00509-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de abril de 2022
Última revisión	11 de abril de 2022
Indicadores de compromiso	
URL redirección	
http://reisdaviau[.]pt/activacion/cuenta-rjol/	
URL sitio falso	
https://www-banc0falabella-cl.happyconnectingtech[.]com/login	
IP	
[27.54.89.134]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00509-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00509-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00510-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2022
Última revisión	12 de abril de 2022
Indicadores de compromiso	
URL redirección	
http://ec2-3-95-188-42.compute-1.amazonaws[.]com/D0190238787912-3/?hash=cG11bm96dkBpbnRlcmlvci5nb3YuY2w=	
URL sitio falso	
https://itautarjeta[.]net/726a292db52f7f5/html/index.php	
IP	
[52.70.212.51]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00510-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00510-01.pdf	

Imagen del mensaje

CSIRT informa phishing con falsa recarga del Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00511-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2022
Última revisión	12 de abril de 2022
Indicadores de compromiso	
URL sitio falso	
https://itau.notificacionrecargacl[.]com/App13799b5/access.php	
IP	
[20.226.60.161]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00511-01/	
https://www.csirt.gob.cl/media/2022/04/8FPH22-00511-01.pdf	

Vulnerabilidades

CSIRT alerta de nueva vulnerabilidad en Microsoft Edge	
Alerta de seguridad cibernética	9VSA22-00614-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de abril de 2022
Última revisión	7 de abril de 2022
CVE	
CVE-2022-1232	
Fabricante	
Microsoft	
Productos afectados	
Microsoft Edge (Chromium-based): 79.0.309.71 a 100.0.1185.29	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00614-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00614-01.pdf	

CSIRT alerta de vulnerabilidades en Mozilla Firefox y Thunderbird	
Alerta de seguridad cibernética	9VSA22-00615-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de abril de 2022
Última revisión	8 de abril de 2022
CVE	
CVE-2022-1097 CVE-2022-28281 CVE-2022-1196 CVE-2022-28282 CVE-2022-28285	CVE-2022-28286 CVE-2022-24713 CVE-2022-28289 CVE-2022-1197
Fabricante	
Mozilla	
Productos afectados	
Firefox, versiones anteriores a la 99. Firefox ESR, versiones anteriores a la 91.8. Thunderbird, versiones anteriores a la 91.8.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00615-01/	
https://www.csirt.gob.cl/media/2022/04/9VSA22-00615-01.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday Abril 2022 de Microsoft	
Alerta de seguridad cibernética	9VSA22-00616-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de abril de 2022
Última revisión	12 de abril de 2022

CVE		
CVE-2022-26790	CVE-2022-26791	CVE-2022-24534
CVE-2022-26789	CVE-2022-26793	CVE-2022-24485
CVE-2022-26786	CVE-2022-26825	CVE-2022-24533
CVE-2022-26917	CVE-2022-26822	CVE-2022-24484
CVE-2022-26916	CVE-2022-26821	CVE-2022-24481
CVE-2022-26915	CVE-2022-26819	CVE-2022-24479
CVE-2022-26831	CVE-2022-26820	CVE-2022-24527
CVE-2022-26828	CVE-2022-26788	CVE-2022-24474
CVE-2022-26827	CVE-2022-26830	CVE-2022-24521
CVE-2022-26824	CVE-2022-26829	CVE-2022-24472
CVE-2022-26823	CVE-2022-26818	CVE-2022-23268
CVE-2022-26812	CVE-2022-26817	CVE-2022-26903
CVE-2022-26802	CVE-2022-26816	CVE-2022-24550
CVE-2022-26807	CVE-2022-26815	CVE-2022-24765
CVE-2022-26803	CVE-2022-26814	CVE-2022-24513
CVE-2022-26801	CVE-2022-26914	CVE-2022-24547
CVE-2022-26787	CVE-2022-26924	CVE-2022-26901
CVE-2022-26796	CVE-2022-26921	CVE-2022-24499
CVE-2022-26798	CVE-2022-26898	CVE-2022-26784
CVE-2022-26797	CVE-2022-26897	CVE-2022-26783
CVE-2022-24549	CVE-2022-26896	CVE-2022-24767
CVE-2022-26919	CVE-2022-24548	CVE-2022-26785
CVE-2022-26811	CVE-2022-24544	CVE-2022-24498
CVE-2022-26810	CVE-2022-24545	CVE-2022-24546
CVE-2022-26808	CVE-2022-24496	CVE-2022-24495
CVE-2022-26918	CVE-2022-24493	CVE-2022-24494
CVE-2022-26809	CVE-2022-24541	CVE-2022-24542
CVE-2022-26813	CVE-2022-24492	CVE-2022-24483
CVE-2022-26910	CVE-2022-24540	CVE-2022-24532
CVE-2022-26907	CVE-2022-24491	CVE-2022-24528
CVE-2022-26911	CVE-2022-24539	CVE-2022-24473
CVE-2022-23292	CVE-2022-24538	CVE-2022-23259
CVE-2022-26904	CVE-2022-24490	CVE-2022-23257
CVE-2022-26826	CVE-2022-24489	CVE-2022-21983
CVE-2022-26832	CVE-2022-24537	CVE-2022-22009
CVE-2022-26920	CVE-2022-24488	CVE-2022-22008
CVE-2022-26795	CVE-2022-24536	CVE-2022-24543
CVE-2022-26794	CVE-2022-24487	CVE-2022-24500
CVE-2022-26792	CVE-2022-24486	CVE-2022-24530

Fabricante
Microsoft
Productos afectados
Azure SDK for .Net
Azure Site Recovery VMWare to Azure
HEVC Video Extension
HEVC Video Extensions
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8
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 Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2016 (32-bit edition)
Microsoft Excel 2016 (64-bit edition)
Microsoft Lync Server 2013 CU10
Microsoft Malware Protection Engine
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
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 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft On-Premises Data Gateway
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)

Microsoft Visual Studio 2019 version 16.7 (includes 16.0 – 16.6)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2022 version 17.1
Skype for Business Server 2015 CU12
Skype for Business Server 2019 CU6
Visual Studio 2019 for Mac version 8.10
Visual Studio Code
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 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 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 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
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, version 20H2 (Server Core Installation) Windows Upgrade Assistant YARP 1.0 YARP 1.1RC
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00616-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00616-01.pdf

CSIRT advierte ante nuevas vulnerabilidades en Google Chrome		
Alerta de seguridad cibernética	9VSA22-00617-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	12 de abril de 2022	
Última revisión	12 de abril de 2022	
CVE		
CVE-2022-1305 CVE-2022-1306 CVE-2022-1307 CVE-2022-1308	CVE-2022-1309 CVE-2022-1310 CVE-2022-1311	CVE-2022-1312 CVE-2022-1313 CVE-2022-1314
Fabricante		
Google		
Productos afectados		
Google Chrome: 70.0.3538.67 a 100.0.4896.75		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00617-01/		
https://www.csirt.gob.cl/media/2022/04/9VSA22-00617-01.pdf		

CSIRT alerta de vulnerabilidades críticas en productos VMware		
Alerta de seguridad cibernética	9VSA22-00618-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	13 de abril de 2022	
Última revisión	13 de abril de 2022	
CVE		
CVE-2022-22954 CVE-2022-22955 CVE-2022-22956	CVE-2022-22957 CVE-2022-22958 CVE-2022-22959	CVE-2022-22960 CVE-2022-22961
Fabricante		
VMware		

Productos afectados
VMware Workspace ONE Access
VMware Identity Manager
VMware vRealize Automation
VMware Cloud Foundation
VMware Suite Lifecycle Manager
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00618-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00618-01.pdf

CSIRT alerta de vulnerabilidades críticas en productos Adobe		
Alerta de seguridad cibernética	9VSA22-00619-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	13 de abril de 2022	
Última revisión	13 de abril de 2022	
CVE		
CVE-2022-24093	CVE-2022-28231	CVE-2022-28257
CVE-2022-24101	CVE-2022-28232	CVE-2022-28258
CVE-2022-24103	CVE-2022-28233	CVE-2022-28259
CVE-2022-24104	CVE-2022-28234	CVE-2022-28260
CVE-2022-27785	CVE-2022-28235	CVE-2022-28261
CVE-2022-24102	CVE-2022-28236	CVE-2022-28262
CVE-2022-27783	CVE-2022-28237	CVE-2022-28263
CVE-2022-27784	CVE-2022-28238	CVE-2022-28264
CVE-2022-27786	CVE-2022-28239	CVE-2022-28265
CVE-2022-27787	CVE-2022-28240	CVE-2022-28266
CVE-2022-27788	CVE-2022-28241	CVE-2022-28267
CVE-2022-27789	CVE-2022-28242	CVE-2022-28268
CVE-2022-27790	CVE-2022-28243	CVE-2022-28269
CVE-2022-27791	CVE-2022-28244	CVE-2022-28270
CVE-2022-27792	CVE-2022-28245	CVE-2022-28271
CVE-2022-27793	CVE-2022-28246	CVE-2022-28272
CVE-2022-27794	CVE-2022-28247	CVE-2022-28273
CVE-2022-27795	CVE-2022-28248	CVE-2022-28274
CVE-2022-27796	CVE-2022-28249	CVE-2022-28275
CVE-2022-27797	CVE-2022-28250	CVE-2022-28276
CVE-2022-27798	CVE-2022-28251	CVE-2022-28277
CVE-2022-27799	CVE-2022-28252	CVE-2022-28278
CVE-2022-27800	CVE-2022-28253	CVE-2022-28279
CVE-2022-27801	CVE-2022-28254	CVE-2022-24105
CVE-2022-27802	CVE-2022-28255	CVE-2022-24098
CVE-2022-28230	CVE-2022-28256	CVE-2022-23205
Fabricante		
Adobe		
Productos afectados		

Adobe Commerce 2.4.3-p1 y anteriores, 2.3.7-p2 y anteriores. Magento Open Source 2.4.3-p1 y anteriores, 2.3.7-p2 y anteriores. Acrobat DC 22.001.20085 y anteriores. Acrobat Reader DC 22.001.20085 y anteriores. Acrobat 2020 20.005.30314 y anteriores (Windows) Acrobat 2020 20.005.30311 y anteriores (macOS) Acrobat Reader 2020 20.005.30314 y anteriores (Windows) Acrobat Reader 2020 20.005.30311 y anteriores (macOS) Acrobat 2017 17.012.30205 y anteriores. Acrobat Reader 2017 17.012.30205 y anteriores. Photoshop 2021 versión 22.5.6 y anteriores. Photoshop 2022 versión 23.2.2 y anteriores. Adobe After Effects 22.2.1 y anteriores, 18.4.5 y anteriores.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00619-01/
https://www.csirt.gob.cl/media/2022/04/9VSA22-00619-01.pdf

Actualidad

Ciberdiccionario

Para muchas personas, la ciberseguridad es un concepto técnico y que sólo algunos conocen. Sin embrago, la realidad es que es un tema que debería ser reconocido por todos los ciudadanos, ya que impacta directamente en cada uno de nosotros, ya sea en el mundo laboral como personal.

Para acercar este concepto y todo aquello que engloba e involucra a la ciberseguridad, el CSIRT de Gobierno presentó el "Ciberdiccionario", una nueva campaña semanal en el que explicaremos brevemente y de forma sencilla algunos términos informáticos con el objetivo de que la ciudadanía conozca y aprenda más sobre la seguridad informática.

Encuéntralo aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario/

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.

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.

- Patricio Alexander Muñoz Bernal
- Jorge Andrés Paredes Flores
- Denes Magliona Halles
- Jorge Ignacio Molina Martínez
- Hugo Alejandro Ovando Puelles
- Gonzalo Venegas Aguirre
- Matías Peña (T3sla)
- María Oyarzún Allendes