CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 201

semana del 5 al 11 de mayo de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

17

IP advertidas en múltiples campañas de phishing y de malware.

URL ADVERTIDAS

25

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

56

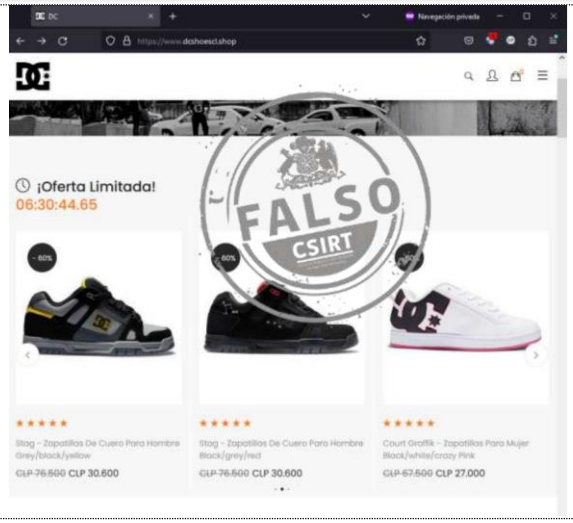
Las mitigaciones son útiles en productos de Fortinet, Google (Chrome) y Microsoft.

CONTENIDO

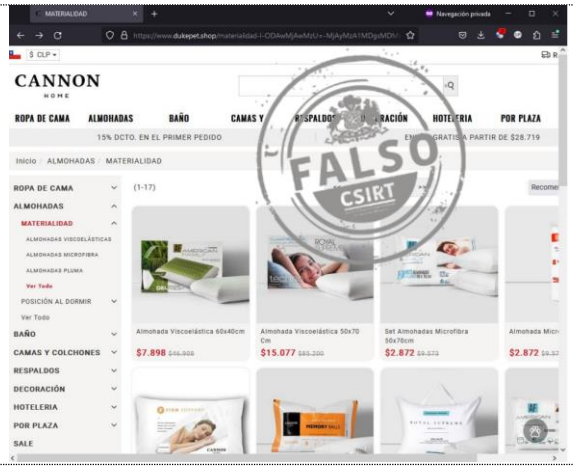
1. Sitios fraudulentos 3
2. Phishing 8
3. Vulnerabilidades 10
4. Concientización 13
5. Recomendaciones y buenas prácticas 15
6. Muro de la Fama 16

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

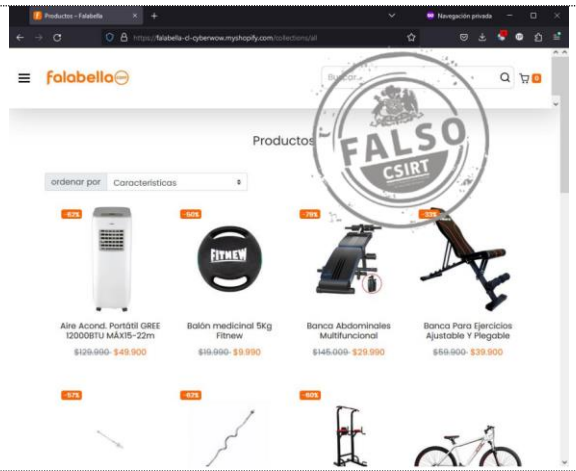
1. Sitios fraudulentos



CSIRT alerta de activación de nuevo sitio fraudulento que suplanta a DC Shoes	
Alerta de seguridad cibernética	8FFR23-01308-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de mayo de 2023
Última revisión	5 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.dcshoescl[.]shop/	
Dirección IP	
[104.21.39.33]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01308-01	

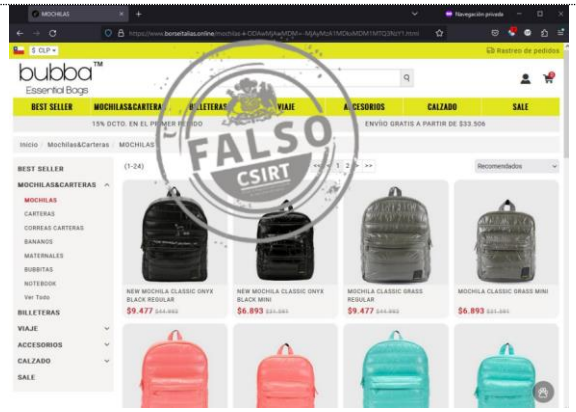


CSIRT alerta de sitio fraudulento que suplanta a Cannon	
Alerta de seguridad cibernética	8FFR23-01309-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de mayo de 2023
Última revisión	8 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.dukepet[.]shop	
Dirección IP	
[23.252.68.239]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01309-01	

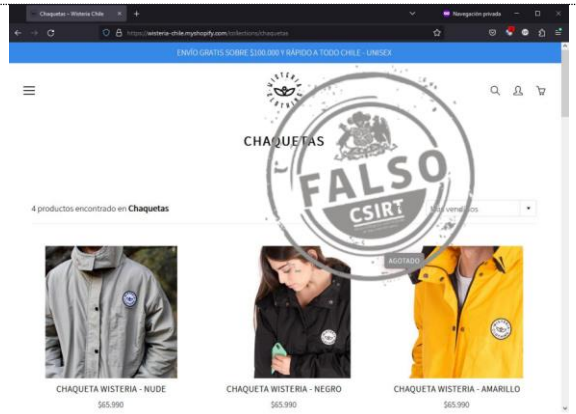


CSIRT alerta de nuevo sitio fraudulento que suplanta a Falabella	
Alerta de seguridad cibernética	8FFR23-01310-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de mayo de 2023
Última revisión	9 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//falabella-cl-cyberwow.myshopify[.]com/	
Dirección IP	
[23.227.38.74]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01310-01	

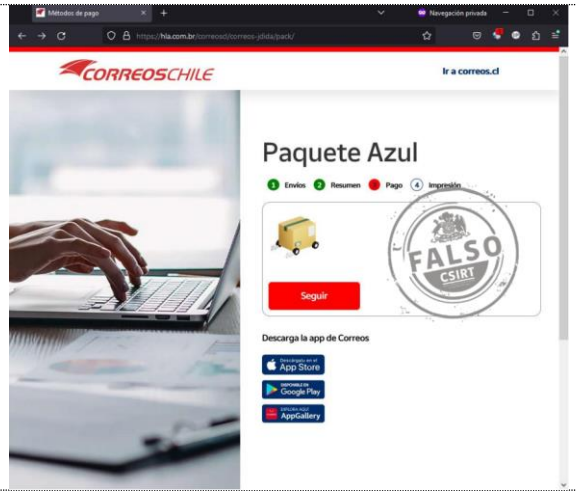
CSIRT alerta de nuevo sitio fraudulento que suplanta a Cannon	
Alerta de seguridad cibernética	8FFR23-01311-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de mayo de 2023
Última revisión	9 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//www.saleshkalmgr[.]online/	
Dirección IP	
[23.252.68.235]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01311-01	



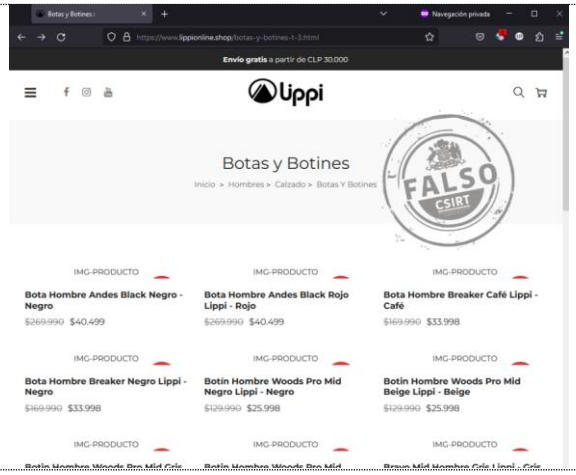
CSIRT alerta de nuevo sitio fraudulento que suplanta a Bubba Bags	
Alerta de seguridad cibernética	8FFR23-01312-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de mayo de 2023
Última revisión	9 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//www.borseitalias[.]online/	
Dirección IP	
[23.252.68.234]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01312-01	



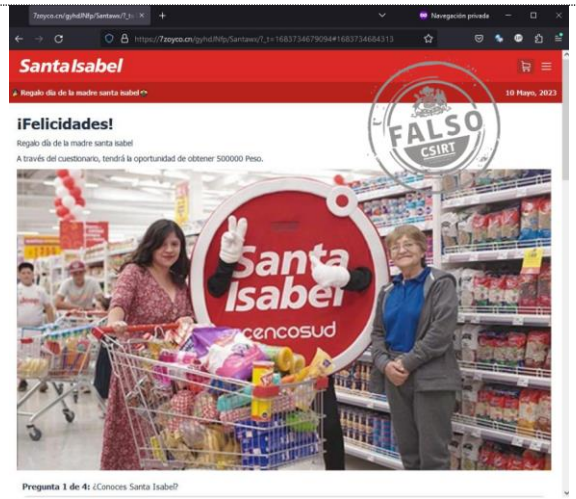
CSIRT alerta de una página fraudulenta que suplanta a Wisteria Clothing	
Alerta de seguridad cibernética	8FFR23-01313-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de mayo de 2023
Última revisión	9 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//wisteria-chile.myshopify[.]com/	
Dirección IP	
[23.227.38.74]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01313-01	



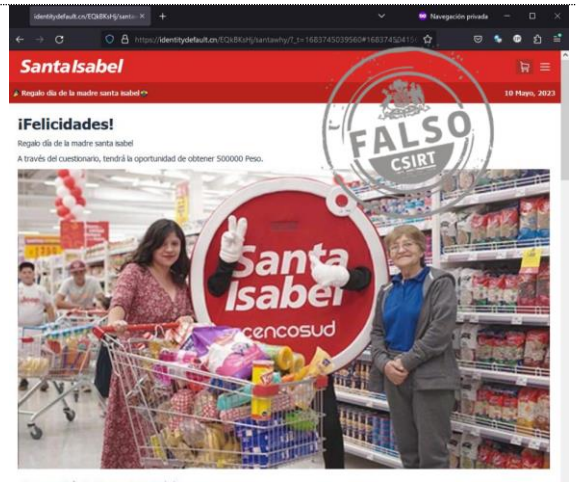
CSIRT alerta de sitio fraudulento que suplanta a CorreosChile	
Alerta de seguridad cibernética	8FFR23-01314-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2023
Última revisión	10 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//hla.com[.]br/correoscl/correos-jdida/pack/	
Dirección IP	
[23.227.38.74]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01314-01	



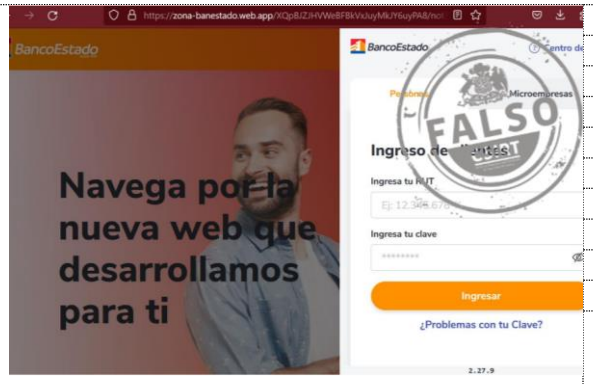
CSIRT alerta de nuevo sitio fraudulento que suplanta a Lippi	
Alerta de seguridad cibernética	8FFR23-01315-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2023
Última revisión	10 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//www.lippionline[.]shop	
Dirección IP	
[172.67.221.142]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01315-01	



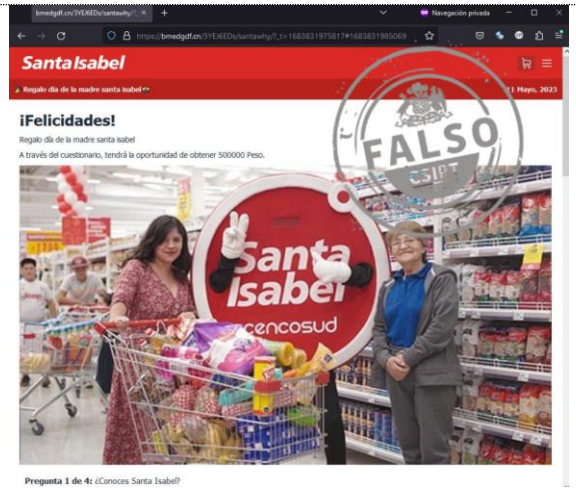
CSIRT alerta de nuevo sitio fraudulento que suplanta a Santa Isabel	
Alerta de seguridad cibernética	8FFR23-01316-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2023
Última revisión	10 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//hurtfulreassure[.]cn/da53AENyWVVVWQRxX2V0eB8TN2MCbx8rN3MrByMiCg1YKToSTgIDOiQJHyJeNQ0JFXsQMFFQHQ1TB2A9DyNKFypPCA?onll1683721273975 https[:]//7zoyco[.]cn/gyhdJNfp/Santawx/?_t=1683734679094#1683734684313	
Dirección IP	
[104.21.21.32]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01316-01	



CSIRT alerta de nuevo sitio fraudulento que suplanta a Santa Isabel	
Alerta de seguridad cibernética	8FFR23-01317-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2023
Última revisión	10 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//presumablyobsessive[.]cn/7763Ql9gXgJceWkAURZrM1ARNnd3MV1XUlhAMXEmOzo_LDRFegcWNEIPNV07EUMXNxYKA1pAMBcPEzYUXXQgNHUbdxA?dfdk1683739592758 https[:]//identitydefault[.]cn/EQkBKsHj/santawhy/?_t=1683745039560#1683745041569	
Dirección IP	
[172.64.204.16]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01317-01	



CSIRT alerta de nuevo sitio fraudulento que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FFR23-01318-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2023
Última revisión	11 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
http[:]//64.227.158.251/5ce0e9faa164d9e8beef007131bae5cd/df60b05ac2256d010a1e14dfc6135d92/610cba09c0b30faf71e7e9acf2cf04c8/ehqdb3b7b1609477124a53b9a72ed331294-cak/?p=est https[:]//zona-banestado.web.app/XQpBJZJHVWeBFBkVxJuyMkJY6uyPA8/not?source=uact&pf_rd_r=3ffgllq5olam	
Dirección IP	
[199.36.158.100]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01318-01	

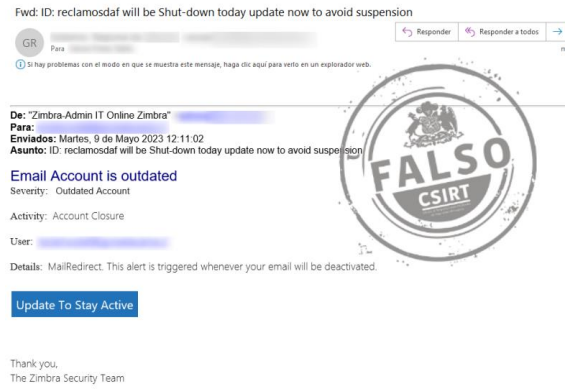


CSIRT alerta de nuevo sitio fraudulento que suplanta a Santa Isabel	
Alerta de seguridad cibernética	8FFR23-01319-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2023
Última revisión	11 de mayo de 2023
Indicadores de compromis9	
URL sitio falso	
https[:]//guncosmetic[.]cn/d9f7An9yeQVKfVFjQDZTWFpHUQ1JXnIKIAl-JgBDPAMJPRQkDxQzHBkTMCoYZxErFzd-Fi5XGjNuISEfIVsXPVBBbT0?rodx1683754047839 https[:]//bmedgdf[.]cn/3YEJ6EDs/santawhy/?_t=1683831975817#1683831985069	
Dirección IP	
[104.21.55.33]	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01319-01	

2. Phishing

CSIRT alerta de nueva campaña de phishing por correo electrónico, que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00805-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de mayo de 2023
Última revisión	9 de mayo de 2023
URL redirección	
https[:]//www.ideaprisma[.]it/online/activacion/cuenta-kzho/	
URL sitio falso	
https[:]//fogaestadosms[.]bio/1683658223/imagenes/_personas/home/default.asp	
Dirección IP	
[104.21.72.4]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00805-01/	

CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00806-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2023
Última revisión	11 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//kacripatito[.]com/1683830140/imagenes/_personas/home/default.asp	
URL redirección:	
https[:]//reachercontact[.]com/activacion/cuenta-bqdc/	
Dirección IP sitio falso	
[98.142.101.90]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00806-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a Zimbra	
Alerta de seguridad cibernética	8FPH23-00807-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2023
Última revisión	11 de mayo de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//6td343iwxptitli4vfaqjqs5xexvzx3lhzuhb7cbt4px2qdlq-ipfs-w3s-link.translate.goog/autozim.html?_x_tr_hp=bafybeig2e&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US&_x_tr_pto=wapp#test@csirt.gob.cl	
Dirección IP sitio falso	
[98.142.101.90]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00807-01/	

3. Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas por Fortinet para varios de sus productos		
Alerta de seguridad cibernética	9VSA23-00829-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	5 de mayo de 2023	
Última revisión	5 de mayo de 2023	
CVE		
CVE-2023-22640	CVE-2022-45859	CVE-2022-45858
CVE-2022-43950	CVE-2022-45860	CVE-2023-27993
CVE-2023-26203	CVE-2023-22637	CVE-2023-27999
Fabricantes		
Fortinet		
Productos afectados		
FortiADC versión 7.2.0		
FortiADC versiones 7.1.0 a 7.1.1		
FortiOS versiones 7.2.0 a 7.2.3		
FortiOS versión 7.0.0 a 7.0.10		
FortiOS versión 6.4.0 a 6.4.11		
FortiOS versión 6.2.0 a 6.2.13		
FortiOS 6.0 todas las versiones		
FortiProxy versión 7.2.0 a 7.2.1		
FortiProxy versión 7.0.0 a 7.0.7		
FortiProxy todas las versiones 2.0, 1.2, 1.1, 1.0		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00829-01/		

CSIRT comparte información de vulnerabilidades parchadas en Google Chrome 113		
Alerta de seguridad cibernética	9VSA23-00830-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	5 de mayo de 2023	
Última revisión	5 de mayo de 2023	
CVE		
CVE-2023-2459	CVE-2023-2463	CVE-2023-2466
CVE-2023-2460	CVE-2023-2464	CVE-2023-2467
CVE-2023-2461	CVE-2023-2465	CVE-2023-2468
CVE-2023-2462		
Fabricantes		
Google		
Productos afectados		
Google Chrome 112		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00830-01/		

CSIRT comparte vulnerabilidades parchadas en su Update Tuesday de mayo 2023	
Alerta de seguridad cibernética	9VSA23-00831-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2023
Última revisión	10 de mayo de 2023

CVE

CVE-2023-24950	CVE-2023-29324	CVE-2023-24941
CVE-2023-24949	CVE-2023-24955	CVE-2023-24901
CVE-2023-24947	CVE-2023-24954	CVE-2023-24940
CVE-2023-24903	CVE-2023-24953	CVE-2023-24900
CVE-2023-29344	CVE-2023-24948	CVE-2023-24939
CVE-2023-29343	CVE-2023-24946	CVE-2023-24899
CVE-2023-29341	CVE-2023-24945	CVE-2023-24898
CVE-2023-29340	CVE-2023-24944	CVE-2023-28290
CVE-2023-29338	CVE-2023-24905	CVE-2023-28283
CVE-2023-29336	CVE-2023-24943	CVE-2023-28251
CVE-2023-29335	CVE-2023-24904	CVE-2023-24932
CVE-2023-29333	CVE-2023-24942	CVE-2023-24881
CVE-2023-29325	CVE-2023-24902	

Fabricantes

Microsoft

Productos afectados

AV1 Video Extension
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft 365 Apps for Enterprise for 64-bit Systems
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 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 Remote Desktop
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Teams
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit editions)
Microsoft Word 2013 Service Pack 1 (64-bit editions)
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
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 20H2 for 32-bit Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 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 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 Sysmon
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00831-01/

4. Concientización

Ciberdiccionario Volumen 36

La edición de esta semana el tradicional Ciberdiccionario del CSIRT de Gobierno comprende los siguientes conceptos: cloaking (en su acepción relacionada con las redes sociales), esteganografía digital, «air gap» y falsos positivos (en su aspecto de ciberseguridad). Todos los volúmenes del ciberdiccionario, junto al resto de nuestras recomendaciones están en: http://csirt.gob.cl/recomendaciones.

Ciberconsejos | Estafas en sitios de compra y venta online

En los sitios de compra y venta de artículos por internet es común que se desarrollen diversas formas de estafa para quedarse ya sea con nuestro dinero, objetos o datos personales. Por eso diseñamos la siguiente edición de Ciberconsejos con algunos indicios que tener en cuenta al momento de usar este tipo de portales: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-compra-venta-online/.

5. 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.

6. 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.

- Agustín Salas Fernández
- Mauricio Alexis Bahamondes González
- Christian Abarca
- María Jesús Pizarro
- Felipe Cifuentes Ramos
- Dennis Armando Juárez Cantellano
- Juan Carlos Rodríguez López
- Nicolás Contador
- Víctor Cofré
- Óscar Guarda Ríos
- Carlos David Escalona
- Christopher Follin Cheuquemán
- Juan Daniel Córdova Luna
- Hernán Francisco Díaz Farías

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.12 16:03:41 -04'00'