Ministerio del Interior y Seguridad Pública

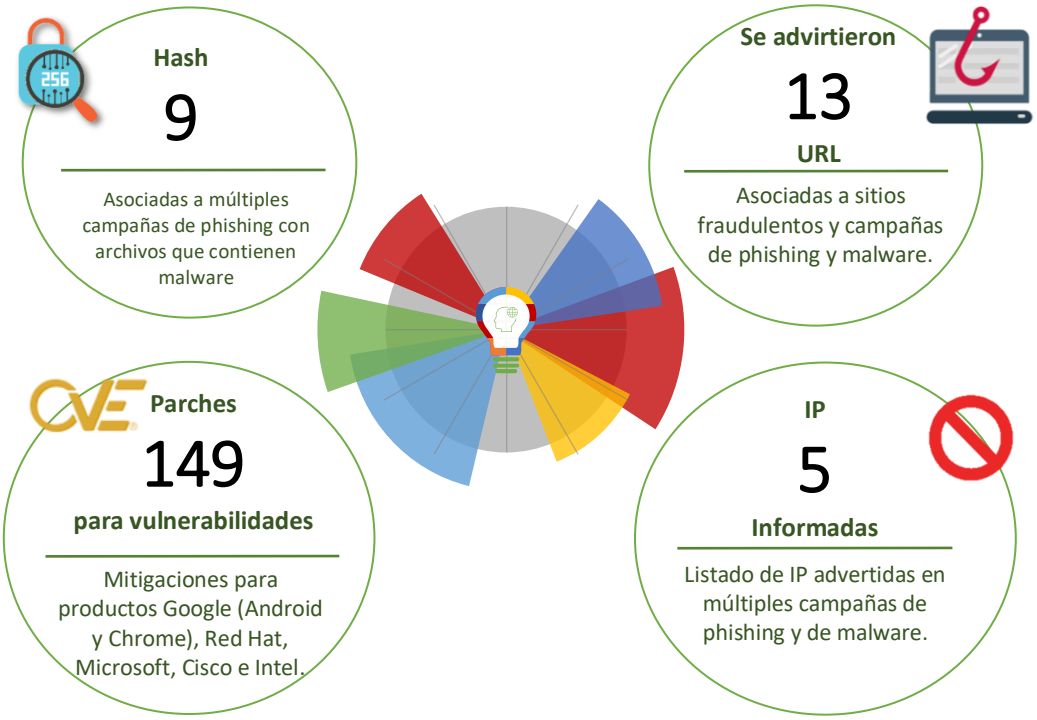
CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

13-05-2022 | Año 4 | N°149

Boletín de Seguridad Cibernética

Semana del 6 al 12 de mayo de 2022

La semana en cifras

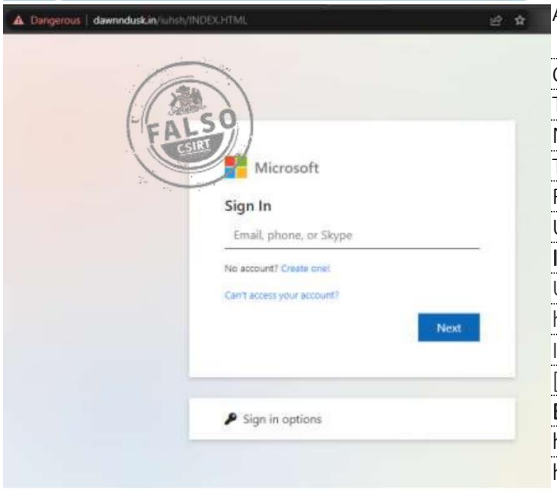


*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Sitios fraudulentos

Imagen del sitio



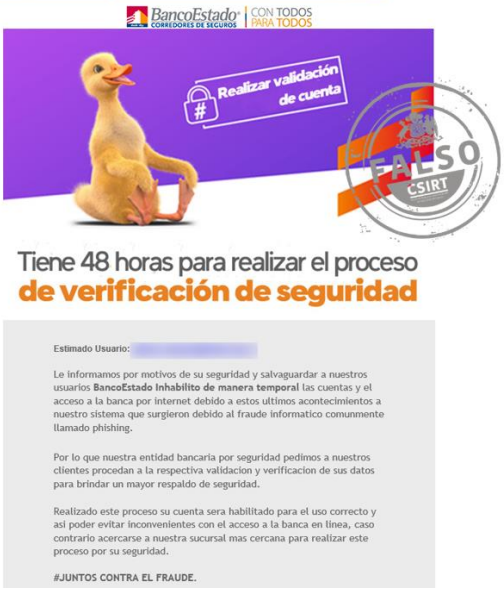
CSIRT informa de sitio fraudulento de Microsoft	
Alerta de seguridad cibernética	8FFR22-01081-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2022
Última revisión	12 de mayo de 2022
Indicadores de compromiso	
URL sitio falso	
hXXps://dawnndusk[.]in/iuhsh/INDEX.HTML	
IP	
[192.185.129.133]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01081-01/	
https://www.csirt.gob.cl/media/2022/05/8FFR22-01081-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing con falsa cuenta suspendida	
Alerta de seguridad cibernética	8FPH22-00521-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	6 de mayo de 2022
Última revisión	6 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXps://kaukaparaiso[.]com/ganador/cuenta-ozli/	
URL sitio falso	
hXXps://kendranew[.]com/sjeudf/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[138.128.170.234]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00521-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00521-01.pdf	

Imagen del mensaje

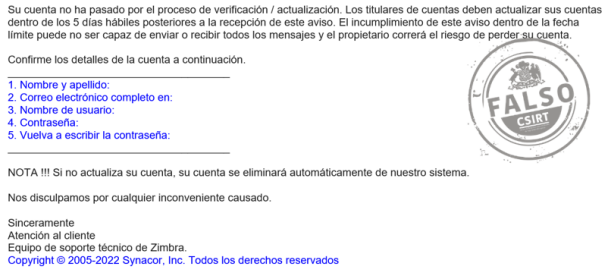


CSIRT advierte phishing con falsa cuenta inhabilitada	
Alerta de seguridad cibernética	8FPH22-00522-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2022
Última revisión	10 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXps://gestionvalpa[.]net/activacion/cuenta-afsn/	
URL sitio falso	
hXXps://kendranew[.]com/pagina/imagenes/comun2008/banca-en-linea-personas.html	
IP	
[138.128.170.234]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00512-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00522-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00523-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2022
Última revisión	11 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXps://bit[.]ly/3kX2384?l=www.santander.cl hXXp://brombalplatform[.]com/disegnatori/bootstrap/enviar03.php?l=1963342191 hXXps://kenhnguoinoitieng[.]com/activacion/cuenta-jiog/	
URL sitio falso	
hXXps://www-santander-cl.innovafurniture.co[.]in/1652213974/Login	
IP	
[135.181.142.217]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00523-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00523-01.pdf	

Imagen del Correo



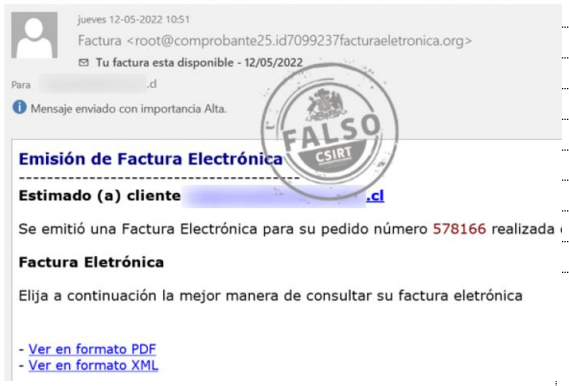
CSIRT informa phishing que suplanta al correo Zimbra	
Alerta de seguridad cibernética	8FPH22-00524-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2022
Última revisión	11 de mayo de 2022
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00524-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00524-01.pdf	

Imagen del mensaje

CSIRT alerta de un phishing que suplanta al Banco Itaú	
Alerta de seguridad cibernética	8FPH22-00525-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de mayo de 2022
Última revisión	11 de mayo de 2022
Indicadores de compromiso	
URL redirección	
hXXp://ec2-3-72-118-141.eu-central-1.compute.amazonaws[.]com/7/5/2/9/2/4/6/0505202246937821393/	
URL sitio falso	
hXXps://productosatualcance[.]com/Appe1bf723/access.php	
IP	
[20.226.60.161]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00525-01/	
https://www.csirt.gob.cl/media/2022/05/8FPH22-00525-01.pdf	

Malware

Imagen del Mensaje



CSIRT advierte malware por falsa factura	
Alerta de seguridad cibernética	2CMV21-00298-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de mayo de 2022
Última revisión	12 de mayo de 2022

Indicadores de compromiso

SHA256

e8fd3f933680a7e12ef159da9eaec83ad885fe2ac9361336dcc6a4ff60dbf3a6
1bb3877853e6b68409b2c8b5c95c8a580fd1504d16a089ffe08d60f8b6dbceb7
bb85e4530ccd6355b3ef3506548b4f513bea844d1af37a69624c9c455521c70f
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
af91374748aca3eefc61de4fedb6595c5ce09e09295c740498238e2b0d25f765
c012d97f6084740fd35b7b927445364e2e2c2e1b5ff0d6836698b4fffb073ef7
3242e0a736ef8ac90430a9f272ff30a81e2afc146fcb84a25c6e56e8192791e4
fd69295a7000348f1dead438a522424db213a1765bbc4679e03040474223a5f2
4a493c35de59fdd1b5f102b2925fea869df8a1510db0cadcd053070a97a9b945

IoC URL

hXXps://www.upec.edu[.]ec/subsitios/ciden/modules/idcliente/
hXXps://fi-ac[.]it/modules/mod_up/.factura/
hXXps://special.arabi21[.]com/russiaWP/serpes0909.goq

Enlaces para revisar el informe:

https://www.csirt.gob.cl/alertas/2cmv22-00298-01/
https://www.csirt.gob.cl/media/2022/05/2CMV22-00298-01-2.pdf

Vulnerabilidades

CSIRT alerta de vulnerabilidades en productos Red Hat		
Alerta de seguridad cibernética	9VSA22-00630-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	6 de mayo de 2022	
Última revisión	6 de mayo de 2022	
CVE		
CVE-2022-29909 CVE-2022-29917 CVE-2022-29911	CVE-2022-29916 CVE-2022-29912 CVE-2022-29914	CVE-2022-29913 CVE-2022-1520 CVE-2022-1271
Fabricante		
Red Hat		
Productos afectados		
Firefox (Red Hat package): 91.2.0-4.el8_1 – 91.8.0-1.el8_5 gzip (Red Hat package): 1.9-10.el8_1 – 1.9-10.el8_2 Red Hat Enterprise Linux Desktop: 7 Red Hat Enterprise Linux for ARM 64 – Extended Update Support: 8.4; ARM 64: 8 Red Hat Enterprise Linux for IBM z Systems – Extended Update Support: 8.4, 8 Red Hat Enterprise Linux for Power, little endian – Extended Update Support: 8.4, little endian: 7, little endian: 8 Red Hat Enterprise Linux for x86_64 – Extended Update Support: 8.4; 8.0 Red Hat Enterprise Linux Server – AUS: 8.4; TUS: 8.2; TUS: 8.4 Red Hat Enterprise Linux Server – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server (for IBM Power LE) – Update Services for SAP Solutions: 8.1 Red Hat Enterprise Linux Server: 7 Red Hat Enterprise Linux Workstation: 7 Thunderbird (Red Hat package): 91.2.0-1.el7_9 – 91.8.0-1.el8_5		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00630-01/		
https://www.csirt.gob.cl/media/2022/05/9VSA22-00630-01.pdf		

CSIRT alerta de vulnerabilidad crítica en Cisco NFVIS	
Alerta de seguridad cibernética	9VSA22-00631-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de mayo de 2022
Última revisión	9 de mayo de 2022
CVE	
CVE-2022-20777 CVE-2022-20779 CVE-2022-20780	
Fabricante	
Cisco	
Productos afectados	
Cisco Enterprise NFVIS	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00631-01/	
https://www.csirt.gob.cl/media/2022/05/9VSA22-00631-01.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday Mayo 2022 de Microsoft		
Alerta de seguridad cibernética	9VSA22-00632-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 de mayo de 2022	
Última revisión	10 de mayo de 2022	
CVE		
CVE-2022-21972	CVE-2022-26935	CVE-2022-29123
CVE-2022-21978	CVE-2022-26936	CVE-2022-29125
CVE-2022-22011	CVE-2022-26937	CVE-2022-29126
CVE-2022-22012	CVE-2022-26938	CVE-2022-29127
CVE-2022-22013	CVE-2022-26939	CVE-2022-29128
CVE-2022-22014	CVE-2022-26940	CVE-2022-29129
CVE-2022-22015	CVE-2022-29102	CVE-2022-29130
CVE-2022-22016	CVE-2022-29103	CVE-2022-29131
CVE-2022-22017	CVE-2022-29104	CVE-2022-29132
CVE-2022-22019	CVE-2022-29105	CVE-2022-29133
CVE-2022-22713	CVE-2022-29106	CVE-2022-29134
CVE-2022-23267	CVE-2022-29107	CVE-2022-29135
CVE-2022-23270	CVE-2022-29108	CVE-2022-29137
CVE-2022-23279	CVE-2022-29109	CVE-2022-29138
CVE-2022-24466	CVE-2022-29110	CVE-2022-29139
CVE-2022-26913	CVE-2022-29112	CVE-2022-29140

CVE-2022-26923	CVE-2022-29113	CVE-2022-29141
CVE-2022-26925	CVE-2022-29114	CVE-2022-29142
CVE-2022-26926	CVE-2022-29115	CVE-2022-29145
CVE-2022-26927	CVE-2022-29116	CVE-2022-29148
CVE-2022-26930	CVE-2022-29117	CVE-2022-29150
CVE-2022-26931	CVE-2022-29120	CVE-2022-29151
CVE-2022-26932	CVE-2022-29121	CVE-2022-30129
CVE-2022-26933	CVE-2022-29122	CVE-2022-30130
CVE-2022-26934		

Fabricante

Microsoft

Productos afectados

.NET 5.0; .NET 6.0; .NET Core 3.1
Microsoft .NET Framework 2.0 Service Pack 2; 3.0 Service Pack 2; 3.5; 3.5.1; 4.6; 4.6.2/4.7/4.7.1/4.7.2; 4.8.
Microsoft 365 Apps for Enterprise for 32-bit and 64-bit Systems
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit & 64-bit)
Microsoft Excel 2016 (32-bit & 64-bit)
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 22 y 23
Microsoft Exchange Server 2019 Cumulative Update 11 y 12
Microsoft Office 2019 (32-bit & 64-bit)
Microsoft Office LTSC 2021 (32-bit & 64-bit)
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft Publisher 2013 Service Pack 1 (32-bit & 64-bit)
Microsoft Publisher 2016 (32-bit & 64-bit)
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
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 (inc. 16.0 – 16.10)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft Visual Studio 2022 version 17.0; 17.1.
Microsoft Word 2013 RT Service Pack 1
Microsoft Word 2013 Service Pack 1 (32-bit & 64-bit)
Microsoft Word 2016 (32-bit & 64-bit)
Remote Desktop client for Windows Desktop
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, ARM64 y x64-based Systems
Windows 10 Version 1909 for 32-bit, ARM64 y x64-based Systems

Windows 10 Version 20H2 for 32-bit, ARM64 y x64-based Systems Windows 10 Version 21H1 32-bit, ARM64 y x64-based Systems Windows 10 Version 21H2 for 32-bit 32-bit, ARM64 y x64-based Systems Windows 11 for ARM64 y 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 y 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 y 2012 (Server Core installation) Windows Server 2012 R2 y 2012 R2 (Server Core installation) Windows Server 2016 y 2016 (Server Core installation) Windows Server 2019 y 2019 (Server Core installation) Windows Server 2022 y 2022 (Server Core installation) Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00632-01/
https://www.csirt.gob.cl/media/2022/05/9VSA22-00632-01.pdf

CSIRT comparte vulnerabilidades de Android Mayo 2022	
Alerta de seguridad cibernética	9VSA22-00633-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de mayo de 2022
Última revisión	10 de mayo de 2022

CVE		
CVE-2021-39662	CVE-2021-39662	CVE-2022-22072
CVE-2022-20004	CVE-2022-0847	CVE-2021-35090
CVE-2022-20005	CVE-2022-20009	CVE-2021-35072
CVE-2022-20007	CVE-2022-20008	CVE-2021-35073
CVE-2021-39700	CVE-2021-22600	CVE-2021-35076
CVE-2022-20113	CVE-2022-20084	CVE-2021-35078
CVE-2022-20114	CVE-2022-20109	CVE-2021-35080
CVE-2022-20116	CVE-2022-20110	CVE-2021-35086
CVE-2022-20010	CVE-2022-22057	CVE-2021-35087
CVE-2022-20011	CVE-2022-22064	CVE-2021-35094

CVE-2022-20115 CVE-2021-39670 CVE-2022-20112	CVE-2022-22065 CVE-2022-22068	CVE-2021-35096 CVE-2021-35116
Fabricante		
Google		
Productos afectados		
Android, versión 12L y anteriores.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00633-01/		
https://www.csirt.gob.cl/media/2022/05/9VSA22-00633-01.pdf		

CSIRT comparte vulnerabilidades de Cisco		
Alerta de seguridad cibernética	9VSA22-00634-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	11 de mayo de 2022	
Última revisión	11 de mayo de 2022	
CVE		
CVE-2022-20764 CVE-2022-20794 CVE-2022-20796 CVE-2022-20785	CVE-2022-20770 CVE-2022-20771 CVE-2022-20734	CVE-2022-20799 CVE-2022-20801 CVE-2022-20753
Fabricante		
Cisco		
Productos afectados		
RV340 Dual WAN Gigabit VPN Routers RV340W Dual WAN Gigabit Wireless-AC VPN Routers RV345 Dual WAN Gigabit VPN Routers RV345P Dual WAN Gigabit POE VPN Routers TelePresence CE Software RoomOS Software in Cloud-Aware On-Premises, que se basa en la nube Secure Endpoint, ex Advanced Malware Protection (AMP) for Endpoints, for Linux Secure Endpoint, ex AMP for Endpoints, for MacOS Secure Endpoint, formerly AMP for Endpoints, for Windows Cisco SD-WAN vManage Software Release 20.6 y 20.7.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00634-01/		
https://www.csirt.gob.cl/media/2022/05/9VSA22-00634-01.pdf		

CSIRT alerta de vulnerabilidades en Intel Optane		
Alerta de seguridad cibernética	9VSA22-00636-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	11 de mayo de 2022	
Última revisión	11 de mayo de 2022	
CVE		
CVE-2021-33077	CVE-2021-33074	CVE-2021-33083
CVE-2021-33078	CVE-2021-33069	CVE-2021-33082
CVE-2021-33080	CVE-2021-33075	
Fabricante		
Intel		
Productos afectados		
Intel Optane SSD DC D4800X Series todas las versiones. Intel Optane SSD DC P4800X/P4801X Series antes de E2010600. Intel Optane SSD P5800X Series anteriores a L3010200. Intel Optane SSD 905P/900P Series todas las versiones. Intel Optane Memory H10 with Solid State Storage Series Intel Optane Memory H20 with Solid State Storage Series		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00636-01/		
https://www.csirt.gob.cl/media/2022/05/9VSA22-00636-01.pdf		

CSIRT alerta de vulnerabilidades en Google Chrome		
Alerta de seguridad cibernética	9VSA22-00637-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	11 de mayo de 2022	
Última revisión	11 de mayo de 2022	
CVE		
CVE-2022-1633	CVE-2022-1636	CVE-2022-1639
CVE-2022-1634	CVE-2022-1637	CVE-2022-1640
CVE-2022-1635	CVE-2022-1638	CVE-2022-1641
Fabricante		
Google		
Productos afectados		
Versiones anteriores a 101.0.4951.64		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00637-01/		
https://www.csirt.gob.cl/media/2022/05/9VSA22-00637-01.pdf		

Actualidad

Ciberconsejos | ¿Cómo prevenir la escalabilidad de privilegios?

La escalabilidad de privilegios es un tipo de ataque con el que los ciberdelincuentes logran, tras acceder sin autorización a un sector relativamente poco sensible de un sistema, alcanzar otros, explotando fallas en la configuración del mismo o vulnerabilidades de software.

Enlace a la campaña: csirt.gob.cl/recomendaciones/ciberconsejos-escalabilidad-de-privilegios.

Ciberdiccionario Volumen 4

La ciberseguridad implica proteger las redes y sistemas de los distintos ataques o peligros que están presentes en el ciberespacio. Las amenazas se pueden presentar de distintas maneras, por lo que siempre se debe estar atento. Para entender algunos de los riesgos, el CSIRT de Gobierno comparte una nueva versión del ciberdiccionario.

Enlace a la campaña: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-4/.

Ciberdiccionario Volumen 5

El CSIRT de Gobierno comparte la 5ta edición del ciberdiccioario, una campaña semanal en el que explicamos brevemente y de forma sencilla algunos términos informáticos con el objetivo de que la ciudadanía conozca y aprenda más sobre la seguridad informática.

Enlace a la campaña: csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-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 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.

- Jerson Valenzuela Campusano
- Abraham Ermann
- Rodrigo Machado Villegas
- Mathias Roco Fernández
- Carlos David Escalona Peraza