CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 5 | N.º 214

semana del 4 al 10 de agosto de 2023

LA SEMANA EN CIFRAS

IP INFORMADAS

14

IP advertidas en múltiples campañas de phishing y de fraude.

URL ADVERTIDAS

16

URL asociadas a sitios fraudulentos y campañas de phishing y malware

PARCHES COMPARTIDOS

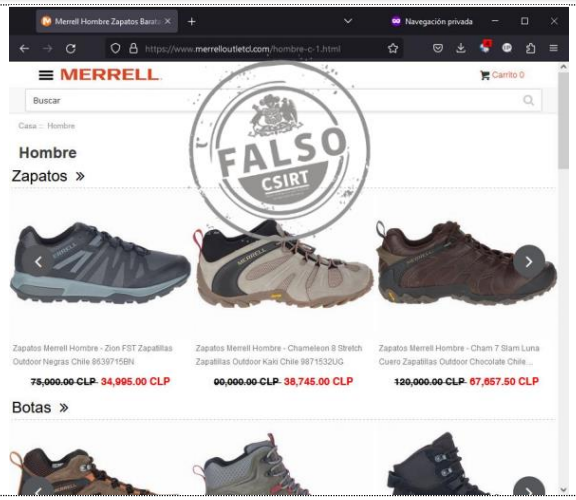
182

Las mitigaciones son útiles en productos de Microsoft, SAP, Adobe, Zoom, Google (Android), Fortinet y Adobe.

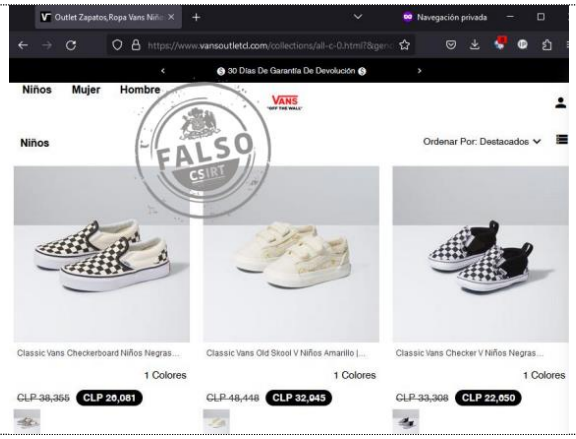
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

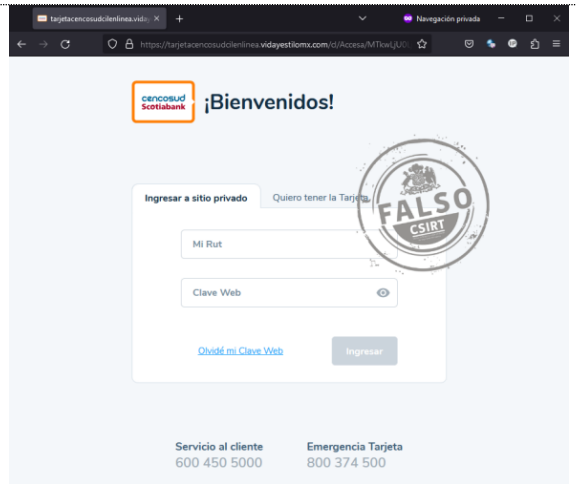
1. Sitios fraudulentos



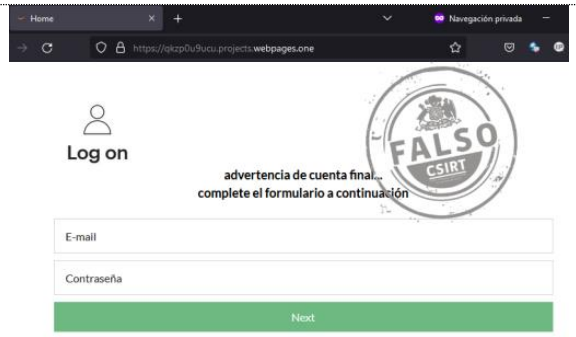
CSIRT alerta de nueva página fraudulenta que suplanta a Merrell	
Alerta de seguridad cibernética	8FFR23-01482-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
TLP	Blanco
Fecha de lanzamiento original	7 agosto, 2023
Última revisión	7 agosto, 2023
Indicadores de compromiso	
URL redirección	
N/A	
URL sitio falso	
https://www.merrelloutletcl[.]com	
Dirección IP	
104.160.5.170	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01482-01/	



CSIRT alerta de un nuevo sitio fraudulento que suplanta a Vans	
Alerta de seguridad cibernética	8FFR23-01483-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
TLP	Blanco
Fecha de lanzamiento original	8 agosto, 2023
Última revisión	8 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://www.vansoutletcl[.]com/	
Dirección IP	
196.196.13.153	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01483-01/	

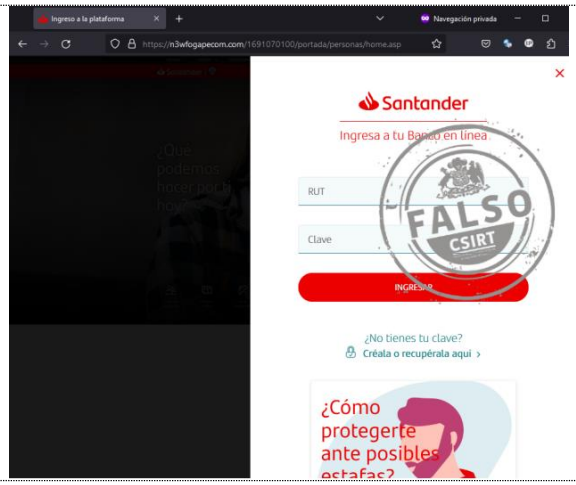


CSIRT alerta de nueva página fraudulenta que suplanta a Tarjetas Cencosud	
Alerta de seguridad cibernética	8FFR23-01484-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
TLP	Blanco
Fecha de lanzamiento original	9 agosto, 2023
Última revisión	9 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://tarjetacencosudcilenlinea.vidayestilomx.com/cl/Accesa/MTkwLjU0LjE2LjEzMw==/Clientes/	
URL redirección	
N/A	
Dirección IP	
146.190.58.89	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01484-01/	



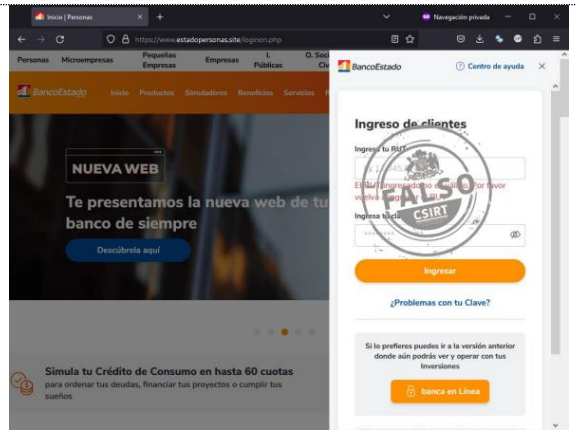
CSIRT alerta de nueva página fraudulenta que suplanta una página de inicio de sesión	
Alerta de seguridad cibernética	8FFR23-01485-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
TLP	Blanco
Fecha de lanzamiento original	10 agosto, 2023
Última revisión	10 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://qkzp0u9ucu.projects.webpages[.]one/	
URL redirección	
N/A	
Dirección IP	
146.190.15.226	
Enlace para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01485-01/	

2. Phishing

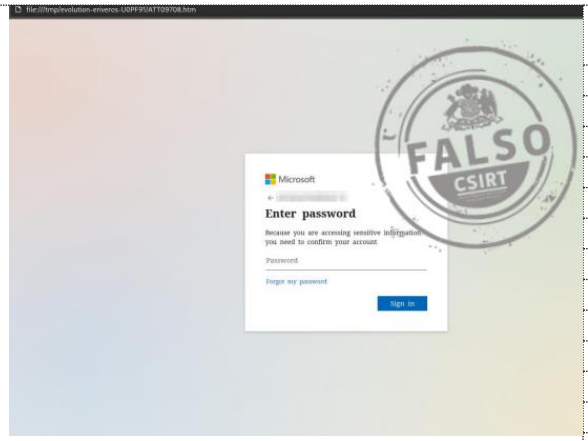


CSIRT alerta de campaña de phishing que suplanta a Banco Santander	
Alerta de seguridad cibernética	8FPH23-00868-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
TLP	Blanco
Fecha de lanzamiento original	7 agosto, 2023
Última revisión	7 agosto, 2023
URL redirección	
https://homefogastadp[.]info/activacion/cuenta-ggqj/	
URL sitio falso	
https://n3wfogapecom[.]com/1691070100/portada/personas/home.asp	
Dirección IP	
[64.37.50.122]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00868-01/	

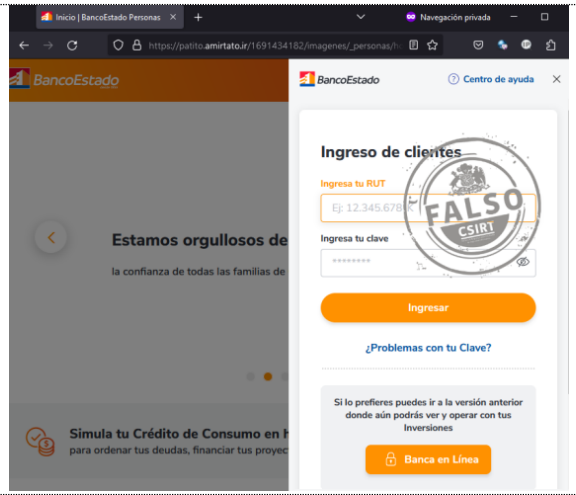
CSIRT alerta de nueva campaña de phishing que engaña con falsa actualización	
Alerta de seguridad cibernética	8FPH23-00869-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
TLP	Blanco
Fecha de lanzamiento original	7 agosto, 2023
Última revisión	7 agosto, 2023
Indicadores de compromiso	
URL redirección	
N/A	
URL sitio falso	
https://cloudflare-ipfs.com/ipfs/bafybeidqqijucohv7taa3ki2r6m2qrk3vean33xw5m5dubglsnc3h5wcl4/fraramzi_cham_e6490.html#test@csirt.gob.cl	
Dirección IP sitio falso	
[104.17.96.13]	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00869-01/	



CSIRT alerta de nueva campaña de phishing que suplanta al Bolsillo Familiar Electrónico y a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00870-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
TLP	Blanco
Fecha de lanzamiento original	7 agosto, 2023
Última revisión	7 agosto, 2023
Indicadores de compromiso	
URL redirección	
https://www.estadopersonas[.]site	
URL sitio falso	
https://www.estadopersonas[.]site/loginon.php	
Dirección IP sitio falso	
172.67.180.206	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00870-01/	



CSIRT alerta de nueva campaña de phishing que suplanta inicio de sesión de Microsoft	
Alerta de seguridad cibernética	8FPH23-00871-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
TLP	Blanco
Fecha de lanzamiento original	7 agosto, 2023
Última revisión	7 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://voipdataentuoercall[.]online/kilokaniga/data.php	
Dirección IP sitio falso	
198.54.117.242	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00871-01/	



CSIRT alerta de nueva campaña de phishing que suplanta a BancoEstado	
Alerta de seguridad cibernética	8FPH23-00872-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
TLP	Blanco
Fecha de lanzamiento original	7 agosto, 2023
Última revisión	7 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://patito.amirtato[.]ir/1691434182/imagenes/_personas/home/default.asp	
URL de redirección	
https://doradobetcontact[.]com/activacion/cuenta-njal/	
Dirección IP sitio falso	
185.126.4.130	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00872-01/	

CSIRT alerta de nueva campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH23-00873-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
TLP	Blanco
Fecha de lanzamiento original	8 agosto, 2023
Última revisión	8 agosto, 2023
Indicadores de compromiso	
URL sitio falso	
https://banco-santander-cl.ifptwe[.]com/1691501034/portada/personas/home.asp	
URL de redirección	
https://bit[.]ly/3KxE2RU?l=www.santander.cl https://www.nationaltreasures[.]co.nz/bancosantander/cuenta-bvri/	
Dirección IP sitio falso	
162.222.225.250	
Enlace para revisar IoC:	
https://www.csirt.gob.cl/alertas/8fph23-00873-01/	

3. Ataques de fuerza bruta

CSIRT alerta de ataques de fuerza bruta contra SMTP	
Alerta de seguridad cibernética	4IIA22-00069-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2023
Última revisión	10 de agosto de 2023
Indicadores de compromiso	
Direcciones IP	
45.129.14.31	
194.55.224.20	
147.78.103.33	
80.76.51.224	
37.139.129.240	
94.156.6.191	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/4iia22-00069-01/	

4. Vulnerabilidades

CSIRT comparte vulnerabilidades parchadas por SAP en su SAP Security Patch Day Agosto 2023

Alerta de seguridad cibernética	9VSA23-00877-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 agosto, 2023
Última revisión	8 agosto, 2023

CVE

CVE-2023-37484	CVE-2023-39437	CVE-2023-39436
CVE-2023-37483	CVE-2023-37490	CVE-2023-37487
CVE-2023-36922	CVE-2023-37491	CVE-2023-37492
CVE-2023-39439	CVE-2023-33993	CVE-2023-39440
CVE-2023-33989	CVE-2023-37488	CVE-2023-36926
CVE-2023-36923	CVE-2023-37486	

Fabricante

SAP

Productos afectados

SAP PowerDesigner 16.7
SAP ECC and SAP S/4HANA (IS-OIL), Versions -600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807.
SAP Commerce, Versions –HY_COM 2105, HY_COM 2205, COM_CLOUD 2211.
SAP NetWeaver (BI CONT ADD ON), Versions –707, 737, 747, 757.
SAP Business One, Version –10.0
SAP Business One (Service Layer), Version –10.0
SAP Business One (B1i Layer), Version –10.0
SAP BusinessObjects Business Intelligence (installer), Versions –420, 430.
SAP Message Server, Versions–KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EX.
SAP Supplier Relationship Management, Versions –600, 602, 603, 604, 605, 606, 616, 617.
SAP NetWeaver Process Integration, Versions-SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50
SAP Commerce (OCC API), Versions-HY_COM 2105, HY_COM 2205, COM_CLOUD 2211.
SAP Supplier Relationship Management, Versions –600, 602, 603, 604, 605, 606, 616, 617.
SAP NetWeaver AS ABAP and ABAP Platform, Versions –SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00877-01/

CSIRT comparte vulnerabilidades publicadas en el Microsoft Update Tuesday de Agosto 2023	
Alerta de seguridad cibernética	9VSA23-00878-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 agosto, 2023
Última revisión	8 agosto, 2023

CVE

ADV230003	CVE-2023-36866	CVE-2023-36914
ADV230004	CVE-2023-36869	CVE-2023-38154
CVE-2023-20569	CVE-2023-36873	CVE-2023-38157
CVE-2023-21709	CVE-2023-36876	CVE-2023-38167
CVE-2023-29328	CVE-2023-36877	CVE-2023-38169
CVE-2023-29330	CVE-2023-36881	CVE-2023-38170
CVE-2023-35359	CVE-2023-36882	CVE-2023-38172
CVE-2023-35368	CVE-2023-36889	CVE-2023-38175
CVE-2023-35371	CVE-2023-36890	CVE-2023-38176
CVE-2023-35372	CVE-2023-36891	CVE-2023-38178
CVE-2023-35376	CVE-2023-36892	CVE-2023-38180
CVE-2023-35377	CVE-2023-36893	CVE-2023-38181
CVE-2023-35378	CVE-2023-36894	CVE-2023-38182
CVE-2023-35379	CVE-2023-36895	CVE-2023-38184
CVE-2023-35380	CVE-2023-36896	CVE-2023-38185
CVE-2023-35381	CVE-2023-36897	CVE-2023-38186
CVE-2023-35382	CVE-2023-36898	CVE-2023-38188
CVE-2023-35383	CVE-2023-36899	CVE-2023-38254
CVE-2023-35384	CVE-2023-36900	CVE-2023-4068
CVE-2023-35385	CVE-2023-36903	CVE-2023-4069
CVE-2023-35386	CVE-2023-36904	CVE-2023-4070
CVE-2023-35387	CVE-2023-36905	CVE-2023-4071
CVE-2023-35388	CVE-2023-36906	CVE-2023-4072
CVE-2023-35389	CVE-2023-36907	CVE-2023-4073
CVE-2023-35390	CVE-2023-36908	CVE-2023-4074
CVE-2023-35391	CVE-2023-36909	CVE-2023-4075
CVE-2023-35393	CVE-2023-36910	CVE-2023-4076
CVE-2023-35394	CVE-2023-36911	CVE-2023-4077
CVE-2023-35945	CVE-2023-36912	CVE-2023-4078
CVE-2023-36865	CVE-2023-36913	

Fabricante

Microsoft

Productos afectados

.NET Core
.NET Framework
ASP .NET
ASP.NET
ASP.NET and Visual Studio
Azure Arc
Azure DevOps
Azure HDInsights
Dynamics Business Central Control
Mariner
Memory Integrity System Readiness Scan Tool
Microsoft Dynamics

	Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Office Microsoft Office Excel Microsoft Office Outlook Microsoft Office SharePoint Microsoft Office Visio Microsoft Teams Microsoft WDAC OLE DB provider for SQL Microsoft Windows Microsoft Windows Codecs Library Reliability Analysis Metrics Calculation Engine Role: Windows Hyper-V SQL Server Tablet Windows User Interface Windows Bluetooth A2DP driver Windows Cloud Files Mini Filter Driver Windows Common Log File System Driver Windows Cryptographic Services Windows Defender Windows Fax and Scan Service Windows Group Policy Windows HTML Platform Windows Kernel Windows LDAP – Lightweight Directory Access Protocol Windows Message Queuing Windows Mobile Device Management Windows Projected File System Windows Reliability Analysis Metrics Calculation Engine Windows Smart Card Windows System Assessment Tool Windows Wireless Wide Area Network Service
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00878-01/

CSIRT comparte información de vulnerabilidad parchada por Fortinet para FortiOS	
Alerta de seguridad cibernética	9VSA23-00879-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 agosto, 2023
Última revisión	10 agosto, 2023
CVE	
CVE-2023-29182	
Fabricante	
Fortinet	
Productos afectados	
FortiOS : 7.0.3 a 6.2.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00879-01/	

CSIRT comparte información de vulnerabilidades parchadas por Zoom		
Alerta de seguridad cibernética	9VSA23-00880-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 agosto, 2023	
Última revisión	10 agosto, 2023	
CVE		
CVE-2023-39209	CVE-2023-39210	CVE-2023-36534
CVE-2023-39214	CVE-2023-39218	CVE-2023-36533
CVE-2023-39213	CVE-2023-39217	CVE-2023-36532
CVE-2023-39212	CVE-2023-39216	CVE-2023-36541
CVE-2023-39211	CVE-2023-36535	CVE-2023-36540
Fabricante		
Zoom		
Productos afectados		
Zoom Client SDK before version 5.15.5		
Zoom Clients for Windows before version 5.14.10		
Zoom Desktop Client before version 5.15.5		
Zoom Mobile App before version 5.14.5		
Zoom Rooms before version 5.14.5		
Zoom VDI Client before version 5.15.2		
Zoom VDI Host and Plugin before version 5.14.5		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00880-01/		

CSIRT comparte vulnerabilidades en el Boletín de Seguridad Android Agosto 2023		
Alerta de seguridad cibernética	9VSA23-00881-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 agosto, 2023	
Última revisión	10 agosto, 2023	
CVE		
CVE-2023-21265	CVE-2023-21279	CVE-2023-21133
CVE-2023-21287	CVE-2023-21283	CVE-2023-21134
CVE-2023-21269	CVE-2023-21288	CVE-2023-21140
CVE-2023-21270	CVE-2023-21289	CVE-2023-21242
CVE-2023-21272	CVE-2023-21292	CVE-2023-21275
CVE-2023-21278	CVE-2023-21280	CVE-2023-21271
CVE-2023-21281	CVE-2023-21284	CVE-2023-21274
CVE-2023-21286	CVE-2023-21282	CVE-2023-21285
CVE-2023-21267	CVE-2023-21273	CVE-2023-21268
CVE-2023-21276	CVE-2023-2096	CVE-2023-21290
CVE-2023-21277	CVE-2023-21132	
Fabricante		
Google		
Productos afectados		
Android. Versiones actualizadas: 11, 12, 12L, 13.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00881-01/		

CSIRT comparte vulnerabilidades en el Boletín de Seguridad Android Agosto 2023	
Alerta de seguridad cibernética	9VSA23-00882-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 agosto, 2023
Última revisión	10 agosto, 2023

CVE

CVE-2023-29320	CVE-2023-38229	CVE-2023-38236
CVE-2023-29299	CVE-2023-38230	CVE-2023-38237
CVE-2023-29303	CVE-2023-38231	CVE-2023-38238
CVE-2023-38222	CVE-2023-38232	CVE-2023-38239
CVE-2023-38223	CVE-2023-38233	CVE-2023-38240
CVE-2023-38224	CVE-2023-38234	CVE-2023-38207
CVE-2023-38225	CVE-2023-38235	CVE-2023-38208
CVE-2023-38226	CVE-2023-38212	CVE-2023-38209
CVE-2023-38227	CVE-2023-38211	CVE-2023-38210
CVE-2023-38228		

Fabricante

Google

Productos afectados

Android. Versiones actualizadas: 11, 12, 12L, 13.

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00881-01/

5. Concientización

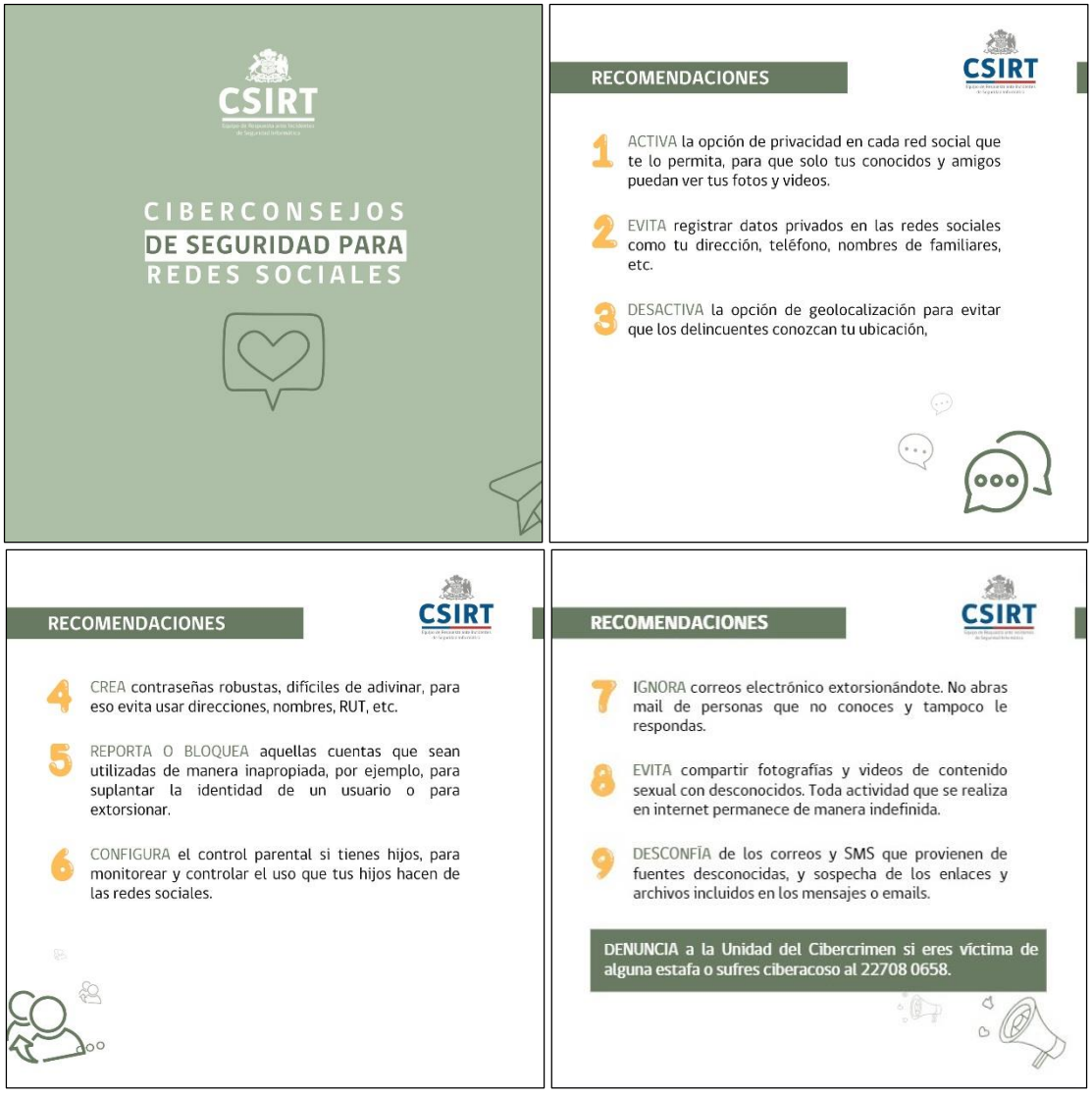
Analista del CSIRT participa en Primer Ejercicio de Ciberseguridad para la Región del Cono Sur en Uruguay

Este 8 de agosto tuvo lugar en Montevideo el Primer Ejercicio de Ciberseguridad para la Región del Cono Sur, organizado por EU CyberNet y Latin America and Caribbean Cyber Competence Centre (LAC4), y financiado por la Unión Europea. Como indica su nombre, la iniciativa contó con participantes de Argentina, Brasil, Paraguay, Uruguay y Chile, y busca fortalecer la ciberseguridad de los organismos públicos en dichas naciones.

Representando a Chile en este ejercicio estuvieron Juan Esteban Moraga, analista del CSIRT del Ministerio del Interior, y el comisario Pedro Rubio Poblete, del Centro Nacional de Ciberseguridad de la Policía de Investigaciones de Chile.. Más información de la jornada: https://www.csirt.gob.cl/noticias/primer-ejercicio-conosur-uruguay/.

Ciberconsejos de seguridad para redes sociales

Todos estamos en las redes sociales (nosotros, el CSIRT de Gobierno, en Instagram, Twitter y LinkedIn, ¡sígannos!) y por eso debemos saber cómo mantenernos más seguros al usarlas. Una manera es siguiendo estos consejos que elaboramos para ustedes, las que esperamos puedan incorporar a sus rutinas digitales y compartir con familiares y amigos: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-rrss/.



Ciberdiccionario Volumen 43

Las definiciones que se suman esta semana al Ciberdiccionario del CSIRT son: geolocalización, pentesting, procesamiento de lenguaje natural y big data. Las imágenes también están disponibles aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-43/.

6. 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.

7. 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.

- Rodolfo Fuentes Arias.
- José David Quezada Rivas.
- Patricio Pérez Cárcamo.
- Hellen Aguilar Aburto.
- Juan Pablo Berríos.
- Javier Ignacio Candia Tapia.
- María José Fuentes.
- Camilo Lazo.
- Miguel Morales Saravia.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.08.11 16:57:52 -04'00'