Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

21-10-2022 | Año 4 | N°172

Boletín de Seguridad Cibernética

Semana del 14 al 20 de octubre de 2022

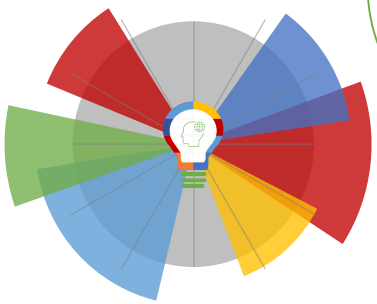
La semana en cifras

Parches

415

para vulnerabilidades

Las mitigaciones son útiles en productos de Google, Aruba, Schneider, Oracle y Apache.



IP

10

Informadas

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

Se advirtieron

20

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

Hash

11

Asociadas a múltiples campañas de phishing con archivos que contienen malware

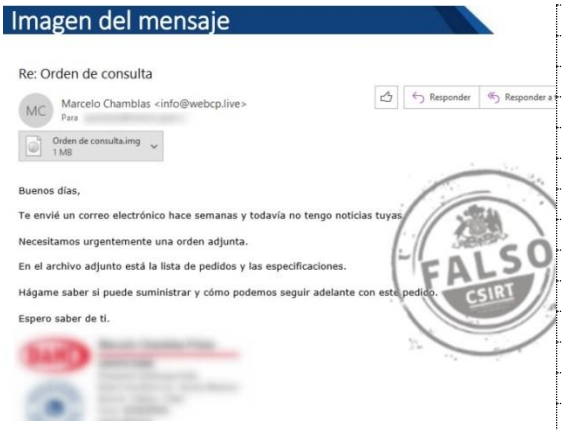
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

Malware

Imagen del Mensaje

CSIRT alerta de campaña de phishing que suplanta a WOM	
Alerta de seguridad cibernética	2CMV22-00359-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2022
Última revisión	17 de octubre de 2022
Indicadores de compromiso	
Asunto	
Re: Pago pendiente	
Correo de Salida	
marialvis.vargas@wom.cl	
SHA256	
Nombre: 00938374.rar SHA256: afd392239889b1539cf39e18fa7f25a7a0fa8fa61fcd93a60ecc807b7716b13f Nombre: 00938374.exe SHA256: c76ab20e58193b2d01eab39426138c5e7fea3e7260523f48546aebaebe703239 Nombre: GZbYa.exe SHA256: e65cf3e55767a5bf458a0d4b8abd5b73e5d21191dab6a2801bf5d04eb5afd4af	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00359-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00359-01.pdf	

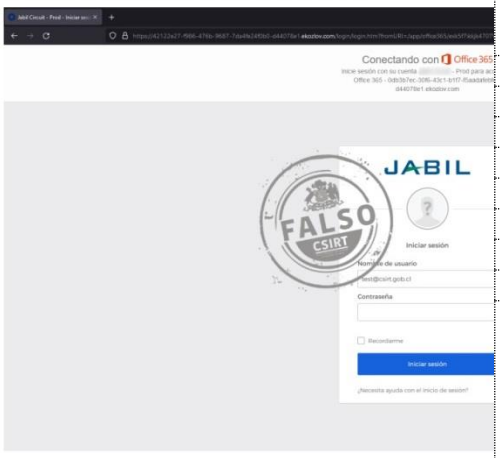


CSIRT alerta ante una campaña de phishing con falsa orden de compra	
Alerta de seguridad cibernética	2CMV22-00360-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2022
Última revisión	18 de octubre de 2022
Indicadores de compromiso	
Asunto	
Re: Orden de consulta	
Correo de Salida	
info@webcp.live	
SHA256	
Nombre: Orden de consulta.img SHA256: 13c91062f56ca1ce356010e822312deecca797f9ce566a338ee65e2669a1ee19 Nombre: Orden de consulta.exe SHA256: 02ef4452bcbeeabc642f85f850ca1a0430a72e2b11a5f32d98c8802f32e68c2f Nombre: RxeJQ.exe SHA256: 9fa64020db23bf493af13047a846c3bce0bb38b55f6cf127d0ec903156d7b442	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00360-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00360-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta a firma de aceros	
Alerta de seguridad cibernética	2CMV22-00361-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2022
Última revisión	19 de octubre de 2022
Indicadores de compromiso	
Asunto	
RE: Solicitud de proforma	
Correo de Salida	
ventas5@acerosryasa.com	
SHA256	
Nombre: ILOTES COT-069pdf.rar SHA256: cb897838f6fbfd6b64eaa2366ad7061fcb4de3f90f7eb9b3f01eaa7d8c0c5a68 Nombre: PILOTES COT-069pdf.exe SHA256: 1be7942fc4b1a55bcc77835df96ec5408aa5ff53fc6ed9d56f7d03c8d3b3ef26 divxc.exe SHA256: cc1f7d86368b3295253c3ee51462767a2c6948ca7925306eedad4b504b1e5926 Nombre: hnazzm.l SHA256: 92e5adfe093a36768506af3eb8e783b9bfb4211ca58d21977a80bc3d1997a0b8 Nombre: fzcyajtz.qb SHA256: ef0fa630bf64b95a32eb8b99454e2968a5d7f1794d1160b47c64f747cc720550	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00361-01/	
https://www.csirt.gob.cl/media/2022/10/2CMV22-00361-01.pdf	

Sitios fraudulentos

Imagen del sitio

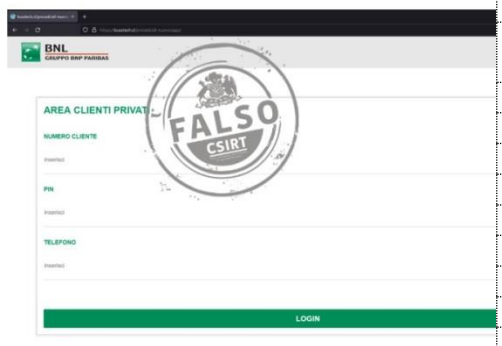


CSIRT alerta ante página fraudulenta que suplanta login de empresa	
Alerta de seguridad cibernética	8FFR22-01124-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2022
Última revisión	17 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://42122e27-f986-476b-9687-7da4fe24f0b0-d44078e1.ekozlov.com/login/login.htm?fromURI=/app/office365/exk5f7ikkjk470TVr0x7/sso/wsfed/passive?login_hint=test@csirt.gob.cl&client-request-id=a0ea3bd7-0473-458d-b600-e15589307f83&username=test@csirt.gob.cl&wa=wsignin1.0&wtrealm=urn:federation:MicrosoftOnline&wctx=estsredirect=2&estsrequest=rQQIARAA42Kw0skoKSkottLXL8gvKknM0cvNTC7KL85PK8nPy8nMS9VLzs_Vyy9Kz0wBsYqEuASuW79aUMzS67qN4WFop0F98ypGZcJG6F9gZHzByDiJSSgxpywzLz4v3SErMSkzByR3i0nQvyjdMyW82C01JbUosSQzP-8RMxaFF1gEXrHwGDBbcXBwCTBIMCgw_GBhXMQKdNOMjn73N_z6bnMnyd-7cy-O4RSrvrFRRGCio1GUc5V7mI9-cYFRRKh-YVCGt0liUWhYYaiBs3elaVaUfoBhRLKtmZXhBDahCWxMp9gYPrAxdrAzzGJnOMDJeICX4Qdf24Wpq462r3nrAQA1	
IP	
[45.82.84.126]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01124-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01124-01.pdf	

Imagen del sitio

CSIRT alerta ante sitio falso que suplanta al banco BNP Paribas	
Alerta de seguridad cibernética	8FFR22-01125-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2022
Última revisión	17 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://cardif-creditoconsumo.alwayson[.]cl/	
IP	
[168.232.167.190]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01125-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01125-01.pdf	

Imagen del sitio



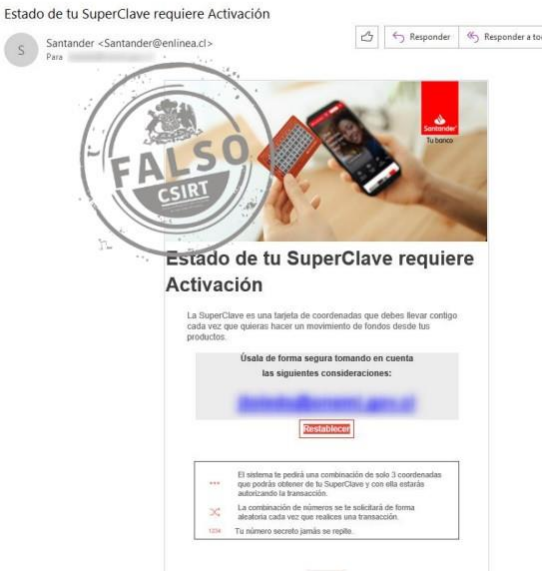
CSIRT alerta ante sitio fraudulento que suplanta la Banca Nazionale del Lavoro	
Alerta de seguridad cibernética	8FFR22-01126-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2022
Última revisión	18 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://busstech[.]cl/procedi/all-nuovo/app/	
IP	
[177.221.140.242]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01126-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01126-01.pdf	

CSIRT alerta ante página fraudulenta que suplanta login de Microsoft

Alerta de seguridad cibernética	8FFR22-01127-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2022
Última revisión	18 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://novedadesdelmundo[.]cl/better/docu10-SELFHOSTING/OUT.html	
IP	
[190.107.176.64]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01127-01/	
https://www.csirt.gob.cl/media/2022/10/8FFR22-01127-01.pdf	

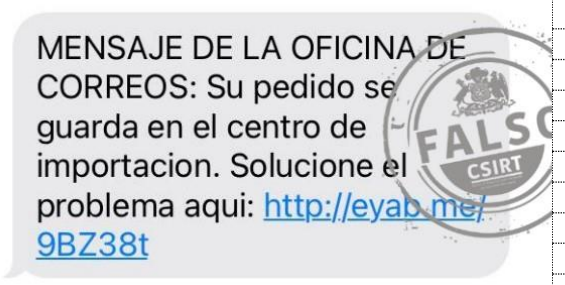
Phishing

Imagen del mensaje



CSIRT alerta ante una nueva campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00618-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2022
Última revisión	14 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://superavances-chile[.]top/santander.php	
URL sitio falso	
https://bancosantander-cl.portal-cl[.]top/1665690260/portada/personas/home.asp	
IP	
[104.21.90.226]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00618-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00618-01.pdf	

Imagen del mensaje

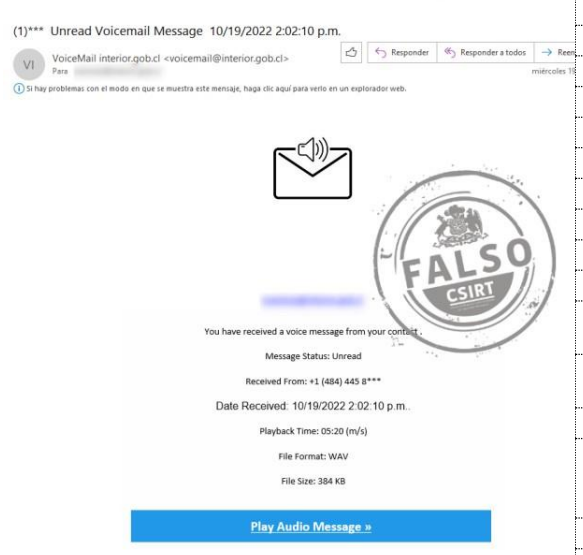


CSIRT alerta ante nueva campaña de smishing	
Alerta de seguridad cibernética	8FPH22-00619-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de octubre de 2022
Última revisión	14 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
http://eyab.me/9BZ38t	
https://salegift[.]live/ips_cl/?cep=wfdoR5Pyf-vtFXsZykPRf2BK3IyZvoBk-WI7voca_p1GoqkinJzEHd5mKhfG-gcQfI7eT7D5BpL7Wwrlgl_jnIRGnHUKgl3rN125GKMcLqrhIx7iWzmJUM20KYpPgUjRVMCs3Cy5gjkhwnRBqrOA41U1VrxZQtrc-qHNTvLftSMqnWu2setX2ukhimHJsM6K97kDEFQr4Xuus01oRGAGoT0xVVzy1CP2jE472OKxQJLjoYf0-B61drkB4lVnPzH2wioeDvSUgM-vvQJNi_Tu5Sjmeu8IJHDZk-MOAuWU82RGa61pRjwma3cquekmHo5i2kZ0O_06j69D09ezv3u5jblItXxaSjR7oq80asu5R3VFysHfRjlGqSktN7AULGcm&lptoken=16f165ce76d700d8189d	
https://www.securepagenow[.]com/?gra=8db9cd0&transaction_id=634976c55f7b680348cd496b&info1=626a924a14c1b679364ef153_2446_2446&info2=2446_2446	
IP	
[5.199.162.244]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00619-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00619-01.pdf	

Imagen del mensaje

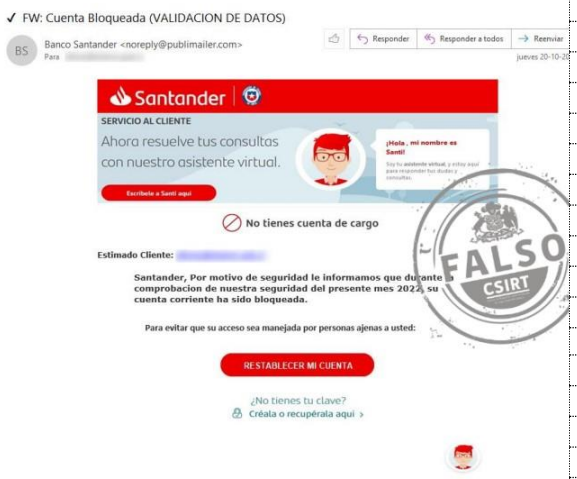
CSIRT alerta de nueva campaña de phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00620-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2022
Última revisión	17 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://bit[.]ly/3EQCe4z?l=www.santander.cl	
http://gimopet[.]vn/storage/framework/testing/enviar02.php?l=1669564352	
https://artsetindustriesinformatiques[.]fr/activacion/cuenta-jkte/	
URL sitio falso	
https://banco.santander.cl.websitedevelopersuk[.]com/1666009834/portada/personas/home.asp	
IP	
[85.92.70.203]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00620-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00620-01.pdf	

Imagen del mensaje



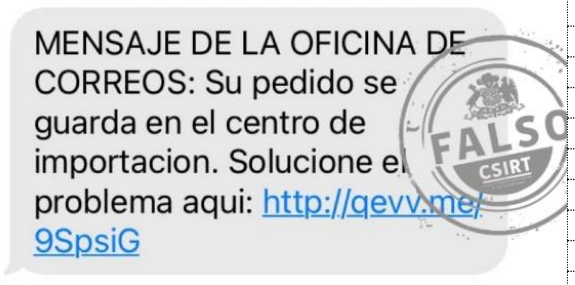
CSIRT alerta ante campaña de phishing con falso mensaje de voz pendiente	
Alerta de seguridad cibernética	8FPH22-00621-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2022
Última revisión	19 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
http://aklab8.com/clickout/7e954854-456e-4de6-9949-84546858e60a#test@csirt.gob.cl&100-22	
https://bafybeicexwnvlkf2cfze66ryuhtglrtfd4s7p7abrqfarxgbmdatq7bh6m.ipfs.w3s.link/gaza	
URL sitio falso	
https://nvlkf2cfze66ryuhtglrtfd4s7p7abrqfarxgbmdatq7bh6m-ipfs-w3s-link.translate.goog/V3.shtml?test@csirt.gob.cl+&_x_tr_hp=bafybeicexw&_x_tr_sl=auto&_x_tr_tl=en-GB&_x_tr_hl=en-GB	
IP	
[142.250.1.132]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00621-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00621-01.pdf	

Imagen del mensaje



CSIRT alerta ante nuevo phishing que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FPH22-00622-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de octubre de 2022
Última revisión	20 de octubre de 2022
Indicadores de compromiso	
URL sitio redirección	
https://surfsantnder[.]info/activacion/cuenta-kand/	
URL sitio falso	
https://elmiguesha.site/1666271662/portada/personas/home.asp	
IP	
[47.87.236.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00622-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00622-01.pdf	

Imagen del mensaje



SIRT alerta por smishing (phishing por SMS) con falso mensaje de «la oficina de correos»	
Alerta de seguridad cibernética	8FPH22-00623-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de octubre de 2022
Última revisión	20 de octubre de 2022
Indicadores de compromiso	
URL sitio falso	
https://salegift[.]live/ips_cl/?cep=sOQHsw6AYJ9vHv8qLpWFAdBe6wckecqtllfq5bu6DyNgJjJvl8RYKw_BnaNybvnIEbWCLleCcT5e0B7XKC3XWuHmmI1AHpEzV6NMT5njxgapAAMTtsGH4lqtF9g-rmlfN5uNCYFvgvcbi-XnHfIqVFezwofDMJ5uFeEc5l-dyAoZixxw2933LHGxfgpRKqK7tOK_JBoEHazmQvlsER6jbair08GeoexRHLrPFjKoypWOTCjy1sGyhKr7Pes0aEkWHHsh1AittyzqN9HeegnQQesqsy-Weup2x_h0RA7GmVRwiiPSFnTGj4I66ZLqaYC7CrR6rTu4rnn9HtcmZZ25aC_4pOTe4shSTCkBfkyei_bh3_JL63qE-8Plg2JFO3cT&lptoken=16726620284503e229f4	
https://www.securepagenow[.]com/?gra=8db9cd0&transaction_id=63516efa4d806e0343afc698&info1=626a924a14c1b679364ef153_2446_2446&info2=2446_2446	
IP	
[47.87.236.153]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00623-01/	
https://www.csirt.gob.cl/media/2022/10/8FPH22-00623-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades en Android para octubre	
Alerta de seguridad cibernética	9VSA22-00724-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2022
Última revisión	17 de octubre de 2022
CVE	
CVE-2022-20419 - CVE-2022-20420 - CVE-2022-20351 CVE-2022-39624 - CVE-2022-39758 - CVE-2022-20415 CVE-2022-20413 - CVE-2022-20418 - CVE-2022-20412 CVE-2022-20416 - CVE-2022-20417 - CVE-2022-39673 CVE-2022-20394 - CVE-2022-20410 - CVE-2022-20425 CVE-2022-1786 - CVE-2022-20421 - CVE-2022-20422 CVE-2022-20423 - CVE-2022-20409 - CVE-2021-0696 CVE-2021-0951 - CVE-2021-0699 - CVE-2022-26471 CVE-2022-26472 - CVE-2022-20430 - CVE-2022-20431 CVE-2022-20432 - CVE-2022-20433 - CVE-2022-20434 CVE-2022-20435 - CVE-2022-20436 - CVE-2022-20437 CVE-2022-20438 - CVE-2022-20439 - CVE-2022-20440 CVE-2022-25720 - CVE-2022-22077 - CVE-2022-25723 CVE-2022-33214 - CVE-2022-33217 - CVE-2022-33218 CVE-2022-25748 - CVE-2022-25718 - CVE-2022-25660 CVE-2022-25661 - CVE-2022-25687 - CVE-2022-25736 CVE-2022-25749	
Fabricante	
Google	
Productos afectados	
Android desde la versión 10.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00724-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00724-01.pdf	

CSIRT alerta de nuevas vulnerabilidades anunciadas por Aruba	
Alerta de seguridad cibernética	9VSA22-00725-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de octubre de 2022
Última revisión	17 de octubre de 2022
CVE	
CVE-2022-37913 CVE-2022-37914 CVE-2022-37915	
Fabricante	
Aruba	
Productos afectados	
Aruba EdgeConnect Enterprise Orchestrator (on-premises) Aruba EdgeConnect Enterprise Orchestrator-as-a-Service Aruba EdgeConnect Enterprise Orchestrator-SP Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators – Orchestrator 9.1.2.40051 y anteriores – Orchestrator 9.0.7.40108 y anteriores – Orchestrator 8.10.23.40009 y anteriores	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00725-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00725-01.pdf	

CSIRT alerta de vulnerabilidades en productos de Schneider Electric		
Alerta de seguridad cibernética	9VSA22-00726-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	18 de octubre de 2022	
Última revisión	18 de octubre de 2022	
CVE		
CVE-2018-7240	CVE-2021-22778	CVE-2022-2463
CVE-2018-7241	CVE-2021-22779	CVE-2022-2464
CVE-2018-7242	CVE-2021-22780	CVE-2022-2465
CVE-2019-6843	CVE-2021-22781	CVE-2022-30790
CVE-2019-6844	CVE-2021-22782	CVE-2022-30552
CVE-2019-6846	CVE-2020-12525	CVE-2022-41666
CVE-2019-6847	CVE-2022-37300	CVE 2022-41667
CVE-2019-6841	CVE-2021-22786	CVE-2022-41668
CVE-2019-6842	CVE-2021-44228	CVE-2022-41669
CVE-2021-22789	CVE-2021-45046	CVE-2022-41670
CVE-2021-22790	CVE-2021-45105	CVE-2022-41671
CVE-2021-22791	CVE-2021-4104	CVE-2022-22727

CVE-2021-22792	CVE-2021-44832	
Fabricantes		
Schneider		
Productos afectados		
EcoStruxure Power Operation 2021 EcoStruxure Power SCADA Operation 2020 EcoStruxure Power SCADA Operation 2020 R2 EcoStruxure Operator Terminal Expert y Pro-face BLUE EcoStruxure Panel Server Box (PAS900) ISaGRAF Workbench for SAGE RTU Apache Log4j Vulnerability (Log4Shell) Modicon PAC Controllers EcoStruxure Control Expert EcoStruxure Process Expert Modicon Controllers M580 y M340 SCADAPack RemoteConnect x70 Modicon Controllers M580 and M340 Modicon PAC Controllers y PLC Simulator para EcoStruxure Control Expert y EcoStruxure Process Expert BadAlloc Vulnerabilities Modicon Controllers Embedded FTP Servers para Modicon PAC Controllers		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00726-01/		
https://www.csirt.gob.cl/media/2022/10/9VSA22-00726-01.pdf		

CSIRT comparte vulnerabilidades corregidas el Chrome 106	
Alerta de seguridad cibernética	9VSA22-00727-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	18 de octubre de 2022
Última revisión	18 de octubre de 2022
CVE	
CVE-2022-3445 - CVE-2022-3446 - CVE-2022-3447 CVE-2022-3448 - CVE-2022-3449 - CVE-2022-3450	
Fabricantes	
Google	
Productos afectados	
Chrome, versiones anteriores a la 106.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00727-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00727-01.pdf	

CSIRT indica vulnerabilidades parchadas en WordPress 6.0.3.	
Alerta de seguridad cibernética	9VSA22-00728-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	19 de octubre de 2022
Última revisión	19 de octubre de 2022
CVE	
Son 15, todas con CVE pendiente.	
Fabricantes	
WordPress	
Productos afectados	
WordPress anteriores al 6.0.3.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00728-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00728-01.pdf	

CSIRT comparte vulnerabilidades del Oracle CPU Octubre 2022		
Alerta de seguridad cibernética	9VSA22-00729-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	19 de octubre de 2022	
Última revisión	19 de octubre de 2022	
CVE		
CVE-2018-1285	CVE-2021-3597	CVE-2022-22971
CVE-2018-1311	CVE-2021-36090	CVE-2022-22971
CVE-2018-18893	CVE-2021-36373.	CVE-2022-22976
CVE-2018-25032	CVE-2021-36374	CVE-2022-22978
CVE-2018-5158	CVE-2021-36483	CVE-2022-23181
CVE-2018-8032	CVE-2021-3737	CVE-2022-23218
CVE-2019-0227	CVE-2021-38153	CVE-2022-23219
CVE-2019-10086	CVE-2021-38604	CVE-2022-23219
CVE-2019-10092	CVE-2021-3918	CVE-2022-23302
CVE-2019-12415	CVE-2021-39275	CVE-2022-23302
CVE-2019-1543	CVE-2021-4034	CVE-2022-23305
CVE-2019-17195	CVE-2021-4048	CVE-2022-23305
CVE-2019-17566.	CVE-2021-40528	CVE-2022-23307
CVE-2019-19956	CVE-2021-40690	CVE-2022-23437
CVE-2019-20388	CVE-2021-4104	CVE-2022-23457
CVE-2019-20838	CVE-2021-41182	CVE-2022-23632
CVE-2019-2904	CVE-2021-41182	CVE-2022-23943
CVE-2019-3855	CVE-2021-41183	CVE-2022-23943
CVE-2019-3856	CVE-2021-41183.	CVE-2022-23990
CVE-2019-3857	CVE-2021-41184	CVE-2022-24675
CVE-2019-3858	CVE-2021-41184	CVE-2022-24728

CVE-2019-3859	CVE-2021-4149.	CVE-2022-24729
CVE-2019-3860	CVE-2021-41495	CVE-2022-24761
CVE-2019-3861	CVE-2021-4178	CVE-2022-24785
CVE-2019-3862	CVE-2021-43396	CVE-2022-24823
CVE-2019-3862	CVE-2021-43527	CVE-2022-24891
CVE-2019-3863	CVE-2021-43797	CVE-2022-25169
CVE-2020-10543	CVE-2021-43859	CVE-2022-25235
CVE-2020-10650	CVE-2021-44228	CVE-2022-25236
CVE-2020-10672	CVE-2021-44790	CVE-2022-25313
CVE-2020-10673	CVE-2021-44832	CVE-2022-25314
CVE-2020-10683	CVE-2022-0778	CVE-2022-25315
CVE-2020-10878	CVE-2022-1154	CVE-2022-25647
CVE-2020-10968	CVE-2022-1292	CVE-2022-25857
CVE-2020-10969	CVE-2022-1586	CVE-2022-26377
CVE-2020-11022	CVE-2022-1587	CVE-2022-27778
CVE-2020-11023	CVE-2022-2047	CVE-2022-27779
CVE-2020-11111	CVE-2022-2048	CVE-2022-27780
CVE-2020-11112	CVE-2022-2068	CVE-2022-27781
CVE-2020-11113	CVE-2022-2097	CVE-2022-27782
CVE-2020-11987	CVE-2022-21123	CVE-2022-27782
CVE-2020-12723	CVE-2022-21125	CVE-2022-28327
CVE-2020-13936	CVE-2022-21127	CVE-2022-28330
CVE-2020-13956	CVE-2022-21166	CVE-2022-28614
CVE-2020-14155	CVE-2022-21540	CVE-2022-28615
CVE-2020-14195	CVE-2022-21541	CVE-2022-29404
CVE-2020-16856	CVE-2022-21549	CVE-2022-29577
CVE-2020-16874	CVE-2022-21587	CVE-2022-29824
CVE-2020-17521	CVE-2022-21589	CVE-2022-29885
CVE-2020-1934	CVE-2022-21590	CVE-2022-30115
CVE-2020-24977	CVE-2022-21591	CVE-2022-30126
CVE-2020-25649	CVE-2022-21592	CVE-2022-30522
CVE-2020-28052	CVE-2022-21593	CVE-2022-30522
CVE-2020-29508	CVE-2022-21594	CVE-2022-30556
CVE-2020-29582	CVE-2022-21595	CVE-2022-31129
CVE-2020-35163	CVE-2022-21596	CVE-2022-31813
CVE-2020-35164	CVE-2022-21597	CVE-2022-31813
CVE-2020-35166	CVE-2022-21598	CVE-2022-32205
CVE-2020-35167	CVE-2022-21599	CVE-2022-32206
CVE-2020-35168.	CVE-2022-21600	CVE-2022-32207
CVE-2020-35169	CVE-2022-21601	CVE-2022-32207
CVE-2020-36189	CVE-2022-21602	CVE-2022-32208
CVE-2020-36518	CVE-2022-21603	CVE-2022-32212
CVE-2020-5421	CVE-2022-21604	CVE-2022-32213
CVE-2020-6950	CVE-2022-21605	CVE-2022-32214
CVE-2020-7595	CVE-2022-21606	CVE-2022-32215
CVE-2020-7712	CVE-2022-21607	CVE-2022-32222
CVE-2020-9484	CVE-2022-21608	CVE-2022-32223
CVE-2020-9492	CVE-2022-21609	CVE-2022-32532
CVE-2020-9546	CVE-2022-21610	CVE-2022-33879

CVE-2020-9547	CVE-2022-21611	CVE-2022-33980
CVE-2020-9548	CVE-2022-21612	CVE-2022-34169
CVE-2021-21290	CVE-2022-21613	CVE-2022-34305
CVE-2021-21295	CVE-2022-21614	CVE-2022-35255
CVE-2021-21409	CVE-2022-21615	CVE-2022-35256
CVE-2021-21707	CVE-2022-21616	CVE-2022-35737
CVE-2021-21708	CVE-2022-21617	CVE-2022-36033
CVE-2021-21783	CVE-2022-21618	CVE-2022-38749
CVE-2021-22118	CVE-2022-21619	CVE-2022-38750
CVE-2021-22144	CVE-2022-21620	CVE-2022-38751
CVE-2021-22946	CVE-2022-21621	CVE-2022-38752
CVE-2021-22947	CVE-2022-21622	CVE-2022-39399
CVE-2021-23450	CVE-2022-21623	CVE-2022-39400
CVE-2021-2351	CVE-2022-21624	CVE-2022-39401
CVE-2021-23926	CVE-2022-21625	CVE-2022-39402
CVE-2021-25122	CVE-2022-21626	CVE-2022-39403
CVE-2021-25329	CVE-2022-21627	CVE-2022-39404
CVE-2021-26291	CVE-2022-21628	CVE-2022-39405
CVE-2021-26690	CVE-2022-21629	CVE-2022-39406
CVE-2021-26691	CVE-2022-21630	CVE-2022-39407
CVE-2021-28163	CVE-2022-21631	CVE-2022-39408
CVE-2021-28164	CVE-2022-21632	CVE-2022-39409
CVE-2021-28165	CVE-2022-21633	CVE-2022-39410
CVE-2021-28490	CVE-2022-21634	CVE-2022-39411
CVE-2021-29425	CVE-2022-21635	CVE-2022-39412
CVE-2021-30129	CVE-2022-21636	CVE-2022-39417
CVE-2021-30639	CVE-2022-21637	CVE-2022-39419
CVE-2021-31805	CVE-2022-21638	CVE-2022-39420
CVE-2021-3426	CVE-2022-21639	CVE-2022-39421
CVE-2021-34429	CVE-2022-21640	CVE-2022-39422
CVE-2021-34798	CVE-2022-21641	CVE-2022-39423
CVE-2021-3517	CVE-2022-2191	CVE-2022-39424
CVE-2021-3518	CVE-2022-22720	CVE-2022-39425
CVE-2021-3537	CVE-2022-22965	CVE-2022-39426
CVE-2021-35515	CVE-2022-22968	CVE-2022-39427
CVE-2021-35516	CVE-2022-22970	CVE-2022-39428
CVE-2021-35517		
Fabricantes		
Oracle		
Productos afectados		
Application Management Pack for Oracle E-Business Suite, version 13.4.1.0.0 Big Data Spatial and Graph Enterprise Manager Base Platform, versions 13.4.0.0, 13.5.0.0 Enterprise Manager for Virtualization, versions 13.4.0.0, 13.5.0.0 Enterprise Manager Ops Center, version 12.4.0.0 JD Edwards EnterpriseOne Orchestrator, versions 9.2.6.4 and prior JD Edwards EnterpriseOne Tools, versions 9.2.6.4 and prior MySQL Connectors, versions 8.0.30 and prior		

MySQL Enterprise Backup, versions 4.1.4 and prior
MySQL Enterprise Monitor, versions 8.0.31 and prior
MySQL Installer, versions 1.6.3 and prior
MySQL Server, versions 5.7.39 and prior, 8.0.30 and prior
MySQL Shell, versions 8.0.30 and prior
MySQL Workbench, versions 8.0.30 and prior
Oracle Access Manager, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Agile Engineering Data Management, version 6.2.1.0
Oracle Agile PLM, version 9.3.6
Oracle Airlines Data Model
Oracle Application Express
Oracle AutoVue, version 21.0.2
Oracle Autovue for Agile Product Lifecycle Management, version 21.0.2
Oracle Banking Enterprise Default Management, version 2.12.0
Oracle Banking Loans Servicing, versions 2.8.0, 2.12.0
Oracle Banking Party Management, version 2.7.0
Oracle Banking Platform, versions 2.7.1, 2.9.0, 2.12.0
Oracle BI Publisher, versions 5.9.0.0, 6.4.0.0.0, 12.2.1.3.0, 12.2.1.4.0
Oracle Business Activity Monitoring(Oracle BAM), versions 12.2.1.3.0, 12.2.1.4.0
Oracle Business Intelligence Enterprise Edition, versions 5.9.0.0, 6.4.0.0
Oracle Business Process Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Coherence, versions 12.2.1.4.0, 14.1.1.0.0
Oracle Commerce Platform, versions 11.3.0-11.3.2
Oracle Communications Billing and Revenue Management, versions 12.0.0.4.0-12.0.0.7.0
Oracle Communications Cloud Native Core Binding Support Function, version 22.3.0
Oracle Communications Cloud Native Core Console, version 22.2.0
Oracle Communications Cloud Native Core Network Exposure Function, versions 22.2.1, 22.3.0
Oracle Communications Cloud Native Core Network Function Cloud Native Environment, versions 1.9.0, 22.1, 22.1.0, 22.2, 22.2.0, 22.2.1
Oracle Communications Cloud Native Core Network Repository Function, version 22.2.2
Oracle Communications Cloud Native Core Policy, version 22.3.0
Oracle Communications Cloud Native Core Security Edge Protection Proxy, versions 22.1.1, 22.2.0, 22.2.1, 22.3.0
Oracle Communications Cloud Native Core Service Communication Proxy, versions 22.2.3, 22.3.1, 22.4.0
Oracle Communications Cloud Native Core Unified Data Repository, versions 22.1.1, 22.2.1, 22.3.0
Oracle Communications Converged Application Server – Service Controller, version 6.2
Oracle Communications Convergence, version 3.0.3.0
Oracle Communications Convergent Charging Controller, versions 6.0.1.0.0, 12.0.1.0.0-12.0.5.0.0
Oracle Communications Data Model, version 12.2.0.1

Oracle Communications Design Studio, version 7.4.2
Oracle Communications Diameter Signaling Router, version 8.6.0.0
Oracle Communications Element Manager, version 9.0
Oracle Communications Evolved Communications Application Server, version 7.1
Oracle Communications Instant Messaging Server, version 10.0.1.6.0
Oracle Communications Interactive Session Recorder, version 6.4
Oracle Communications Messaging Server, version 8.1
Oracle Communications MetaSolv Solution, version 6.3.1
Oracle Communications Network Charging and Control, versions 6.0.1.0.0, 12.0.1.0.0-12.0.5.0.0
Oracle Communications Order and Service Management, versions 7.3, 7.4
Oracle Communications Policy Management, version 12.6.0.0.0
Oracle Communications Pricing Design Center, versions 12.0.0.4.0-12.0.0.7.0
Oracle Communications Services Gatekeeper, version 7.0.0.0.0
Oracle Communications Session Border Controller, versions 8.4, 9.0, 9.1
Oracle Communications Session Report Manager, version 9.0
Oracle Communications Unified Assurance, versions prior to 5.5.7.0.0, 6.0.0.0.0
Oracle Communications User Data Repository, versions 12.4.0, 12.6.0, 12.6.1
Oracle Communications WebRTC Session Controller, versions 7.2.0, 7.2.1
Oracle Data Integrator, version 12.2.1.4.0
Oracle Database Server, versions 19c, 21c
Oracle Documaker Enterprise Edition, versions 12.6-12.7
Oracle E-Business Suite, versions 12.2.3-12.2.11
Oracle Enterprise Data Quality, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Enterprise Operations Monitor, versions 4.4, 5.0
Oracle Essbase, version 21.3
Oracle Financial Services Analytical Applications Infrastructure, versions 8.0.7.0-8.1.0.0, 8.1.1.0, 8.1.2.0, 8.1.2.1
Oracle Financial Services Behavior Detection Platform, versions 8.0.7.2, 8.0.8.1, 8.1.1.0, 8.1.1.1, 8.1.2.0, 8.1.2.1, 8.1.2.2
Oracle Financial Services Enterprise Case Management, versions 8.0.7.3, 8.0.8.2, 8.1.1.0, 8.1.1.1, 8.1.2.0, 8.1.2.1, 8.1.2.2
Oracle Financial Services Model Management and Governance, versions 8.0.8.0, 8.1.0.0, 8.1.1.0
Oracle Financial Services Trade-Based Anti Money Laundering Enterprise Edition, versions 8.0.7.0, 8.0.8.0
Oracle GoldenGate, version 19c
Oracle GraalVM Enterprise Edition, versions 20.3.7, 21.3.3, 22.2.0
Oracle Healthcare Data Repository, versions 8.1.1, 8.1.2, 8.1.3
Oracle Healthcare Foundation, versions 8.1, 8.2
Oracle Healthcare Master Person Index, versions 5.0.0-5.0.3
Oracle Healthcare Translational Research, version 4.1
Oracle Hospitality Cruise Fleet Management System, version 9.1.5
Oracle Hospitality Cruise Shipboard Property Management System,

versions 20.2.0, 20.2.2
Oracle Hospitality Suite8, versions 8.10.2, 8.11.0, 8.12.0, 8.13.0, 8.14.0
Oracle HTTP Server, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Hyperion Infrastructure Technology, version 11.2.9
Oracle Identity Management Suite, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Insurance Insbridge Rating and Underwriting, versions 5.2.0, 5.4.0-5.6.2
Oracle Java SE, versions 8u341, 8u345-perf, 11.0.16.1, 17.0.4.1, 19
Oracle MapViewer, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Middleware Common Libraries and Tools, versions 12.2.1.3.0, 12.2.1.4.0
Oracle NoSQL Database
Oracle Outside In Technology, version 8.5.6
Oracle Retail Assortment Planning, version 16.0.3
Oracle Retail Back Office, version 14.1
Oracle Retail Central Office, version 14.1
Oracle Retail Customer Insights, versions 15.0.2, 15.2, 16.0.2
Oracle Retail Customer Management and Segmentation Foundation, versions 17.0, 18.0, 19.0
Oracle Retail EFTLink, versions 20.0.1, 21.0.0
Oracle Retail Fiscal Management, version 14.2
Oracle Retail Merchandising System, versions 14.1.3.2, 15.0.3.1, 19.0.1
Oracle Retail Point Of Service, version 14.1
Oracle Retail Predictive Application Server, versions 14.1.3.47, 15.0.3.116, 16.0.3.260
Oracle Retail Returns Management, version 14.1
Oracle Retail Sales Audit, version 19.0.1
Oracle Retail Service Backbone, versions 14.1.3.2, 15.0.3.1, 16.0.3
Oracle SD-WAN Aware, version 9.0.1.3.0
Oracle SD-WAN Edge, versions 7.0.7, 9.1.1.2.0
Oracle Secure Backup, versions prior to 18.1.0.2.0
Oracle SOA Suite, versions 12.2.1.3.0, 12.2.1.4.0
Oracle Solaris, version 11
Oracle Solaris Cluster, version 4
Oracle SQL Developer
Oracle TimesTen In-Memory Database
Oracle Transportation Management, versions 6.4.3, 6.5.1
Oracle Utilities Testing Accelerator, versions 6.0.0.1.3, 6.0.0.2.4, 6.0.0.3.3, 7.0.0.0.0
Oracle VM VirtualBox, versions prior to 6.1.40
Oracle WebCenter Content, version 12.2.1.3.0
Oracle WebCenter Portal, versions 12.2.1.3.0, 12.2.1.4.0
Oracle WebCenter Sites, versions 12.2.1.3.0, 12.2.1.4.0
Oracle WebLogic Server, versions 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0
PeopleSoft Enterprise Common Components, version 9.2
PeopleSoft Enterprise PeopleTools, versions 8.58, 8.59, 8.60
Primavera Gateway, versions 18.8.0-18.8.15, 19.12.0-19.12.14, 20.12.0-20.12.9, 21.12.0-21.12.7
Primavera Unifier, versions 18.8, 19.12, 20.12, 21.12

Siebel Applications, versions 22.8 and prior
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00729-01/
https://www.csirt.gob.cl/media/2022/10/9VSA22-00729-01.pdf

CSIRT alerta de vulnerabilidad crítica en Apache Commons Text	
Alerta de seguridad cibernética	9VSA22-00730-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	20 de octubre de 2022
Última revisión	20 de octubre de 2022
CVE	
CVE-2022-42889	
Fabricantes	
Apache	
Productos afectados	
Apache Commons Text anteriores a la versión 1.10.0.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00730-01/	
https://www.csirt.gob.cl/media/2022/10/9VSA22-00730-01.pdf	

Ataques de Fuerza Bruta

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP) para suplantar a los remitentes originales para depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

IP	Etiqueta de Sistema Autónomo	Nombre sistema autónomo	Documento
85.31.46.85	AS 211252	Delis LLC	4IIA22-00053-01
103.153.76.160	AS 135905	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	4IIA22-00053-01
192.227.128.152	AS 36352	AS-COLOCROSSING	4IIA22-00053-01
37.139.128.231	AS 211252	Delis LLC	4IIA22-00053-01
85.209.134.184	AS 211252	Serverion_BV-NET	4IIA22-00053-01
103.145.254.90	AS 135905	VIETNAM POSTS AND TELECOMMUNICATIONS GROUP	4IIA22-00053-01

Actualidad

Alerta de Seguridad Cibernética | Fin de vida de servidores VMware ESXi 6.5 y 6.7

Desde el Equipo de Repuesta a Incidentes de Seguridad Informática del Ministerio del Interior, CSIRT de Gobierno, informamos a todos los actores del ciberespacio nacional que ocupen servidores VMware ESXi 6.5 y 6.7, que estos han alcanzado su fin de vida este 15 de octubre, y que ya no recibirán actualizaciones de seguridad desde VMware.

Dado esto, es recomendable que las organizaciones que aún operen estos servidores implementen versiones más modernas y que continúen con el respaldo de actualizaciones periódicas.

Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00085-01/

Alerta de Seguridad Cibernética | Llamado a actualizar Windows 10 a 21H2 para mantener soporte

Desde el Equipo de Repuesta a Incidentes de Seguridad Informática del Ministerio del Interior, CSIRT de Gobierno, llamamos a todos los actores del ciberespacio nacional que ocupen el sistema operativo Windows, a actualizar a Windows 11 o, si no es factible aún y se requiere usar Windows 10, actualizar el sistema operativo a su versión 21H2.

Lo anterior, debido a que Microsoft informó el fin de su soporte a la versión 21H1 de Windows 10 para este 13 de diciembre, mientras la variante 21H2 tendrá soporte hasta el 13 de junio de 2023.

Detalles: https://www.csirt.gob.cl/noticias/10cnd22-00086-01/

Mes de la Ciberseguridad: Cuida tu privacidad

Gracias a Internet, hoy podemos comunicarnos, trabajar, estudiar, compartir información, entre otros beneficios, pero debes ser cuidadoso con lo que publicas y proteger tus dispositivos (como smartphones, tablets y computadores), con el fin de evitar el robo de datos y resguardar tu privacidad. ¿Cómo te puedes cuidar? Puedes seguir los ciberconsejos del CSIRT de Gobierno: https://www.csirt.gob.cl/recomendaciones/mes-ciberseguridad/

Ciberdiccionario Volumen 20

En la edición número 20, compartimos nuevas definiciones en nuestro ciberdiccionario. En esta ocasión, explicamos qué es copia de seguridad, criptografía, dominio web y gusano informático. Puede verlos también aquí: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-20/.

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 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.

- Fabián Stuardo
- Carlos de la Fuente
- Felipe Honores
- Claudio Pedrero
- Juan Pablo Mellado
- Ignacio Tello
- Javier Ignacio Candia
- Nicolás Cilveti