CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

BOLETÍN DE SEGURIDAD CIBERNÉTICA

Año 4 | N.º 185

SEMANA DEL 13 AL 19 de enero

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

416

Las mitigaciones son útiles en productos de Cisco, Oracle, Mozilla y Juniper Networks.

IP INFORMADAS

15

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

URL ADVERTIDAS

29

Asociadas a sitios fraudulentos y campañas de phishing y malware

HASH REPORTADOS

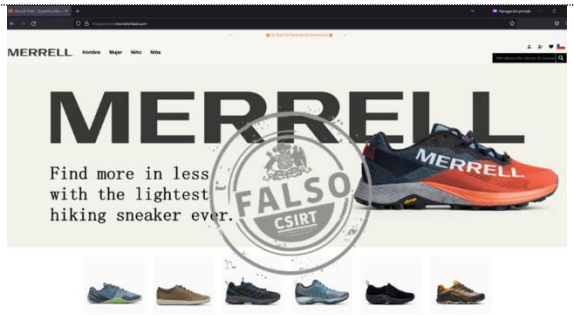
4

Asociadas a múltiples campañas de phishing con archivos que contienen malware

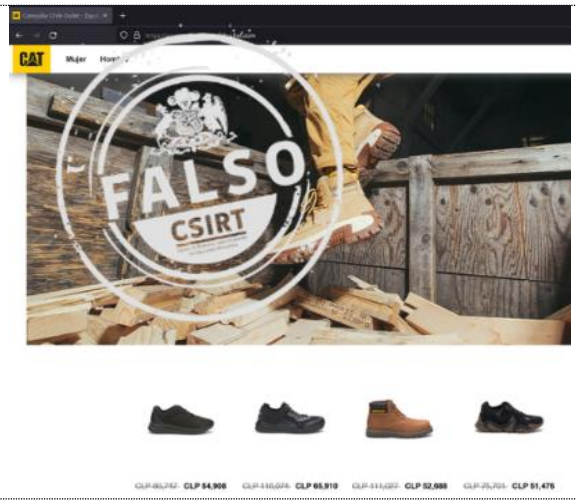
CONTENIDO

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

1. Sitios fraudulentos



CSIRT alerta de sitio falso que suplanta a Merrell	
Alerta de seguridad cibernética	8FFR23-01198-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2023
Última revisión	17 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.merrellchilecl[.]com/	
Dirección IP	
[196.245.238.119]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01198-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01198-01.pdf	

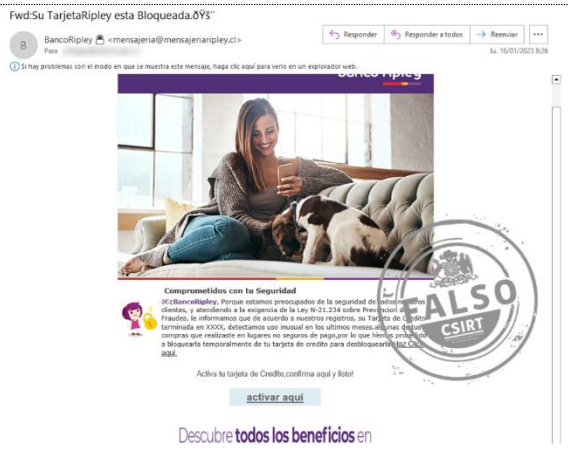


CSIRT alerta de un sitio falso que suplanta a Caterpillar	
Alerta de seguridad cibernética	8FFR23-01199-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2023
Última revisión	17 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.caterpillarchile-outlet[.]com/	
Dirección IP	
[196.240.207.45]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01199-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01199-01-1.pdf	

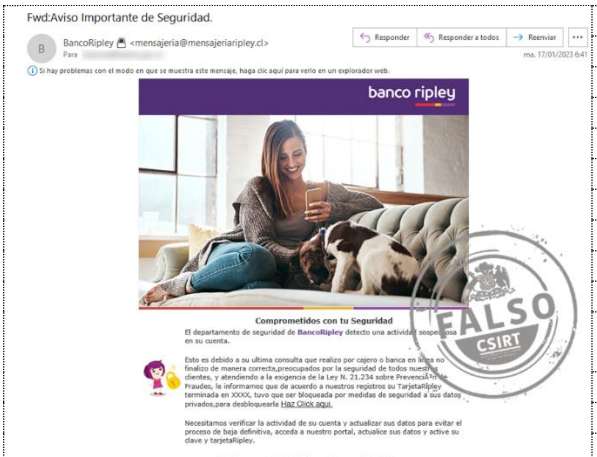
CSIRT alerta de sitio fraudulento que suplanta a Lafuma	
Alerta de seguridad cibernética	8FFR23-01200-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2023
Última revisión	17 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.lafumachile[.]com/	
Dirección IP	
[196.244.47.154]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr23-01200-01/	
https://www.csirt.gob.cl/media/2023/01/8FFR23-01200-01.pdf	

2. Phishing

CSIRT alerta ante nueva campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00712-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2023
Última revisión	16 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3W3lbRL?l=www.bancoripley.cl	
https[:]//sam-tech[.]jp/bancoripley/cuenta-qiec/	
URL sitio falso	
https://web.bancoriipley-cl.awadgallery.co.uk/1673623426/login	
Dirección IP	
[23.88.71.133]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00712-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00712-01.pdf	

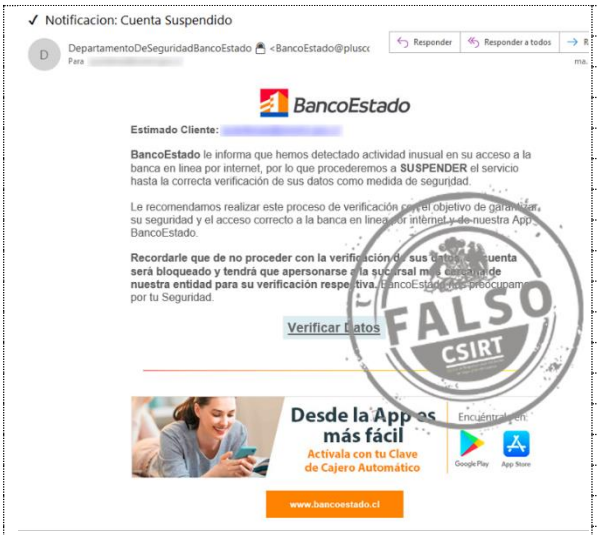


CSIRT alerta ante una nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00713-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2023
Última revisión	16 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3XgwtDN?l=www.bancoripley.cl https[:]//sam-tech[.]jp/bancoripley/cuenta-gphc/	
URL sitio falso	
http[:]//web.bancoripley.cl.archersbodyworks[.]com.au/1673873742/login	
Dirección IP	
[203.28.48.11]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00713-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00713-01.pdf	



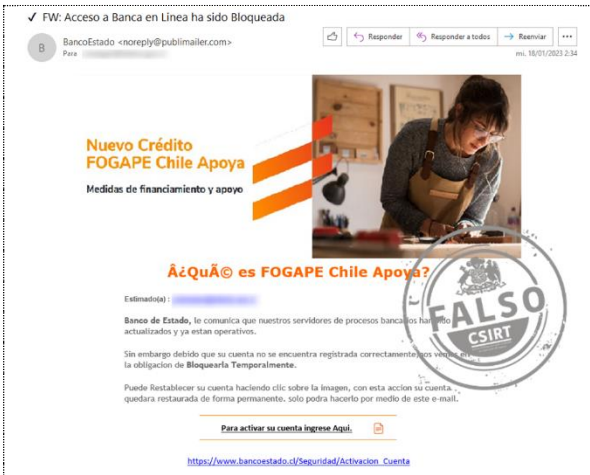
CSIRT alerta de nueva campaña de phishing, que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00714-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de enero de 2023
Última revisión	17 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//bit[.]ly/3GKdr1C?l=www.bancoripley.cl https[:]//sam-tech[.]jp/bancoripley/cuenta-ilah/	
Dirección IP	
[185.45.66.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00714-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00714-01.pdf	

CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00715-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2023
Última revisión	18 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-qvqk/	
URL sitio falso	
https[:]//smschilestado.info/1673968691/imagenes/_personas/home/default.asp	
Dirección IP	
[202.89.39.41]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00715-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00715-01.pdf	



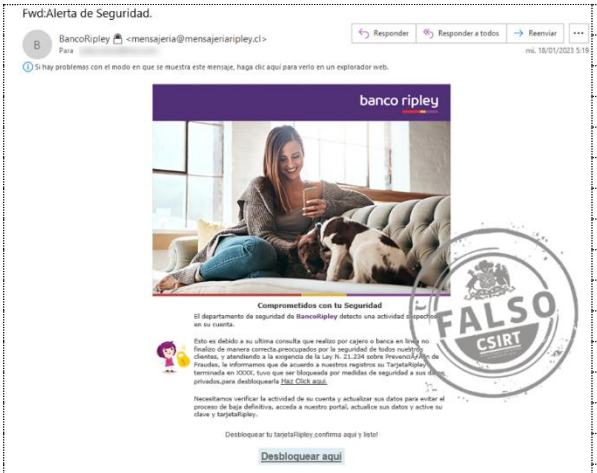
CSIRT informa de una nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00716-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2023
Última revisión	18 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//www.alpavillanew[.]top/activacion/cuenta-fdow/	
URL sitio redirección	
https[:]//springpatito[.]info/1673979528/imagenes/_personas/home/default.asp	
Dirección IP	
[172.67.163.158]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00716-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00716-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta a Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00717-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2023
Última revisión	18 de enero de 2023
Indicadores de compromiso	
URL sitio redirección	
https[:]//xtraillconver[.]com/activacion/cuenta-vtqz/	
URL sitio falso	
https[:]//springpatito[.]info/1673440791/imagenes/_personas/home/default.asp	
Dirección IP	
[185.45.66.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00717-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00717-01.pdf	



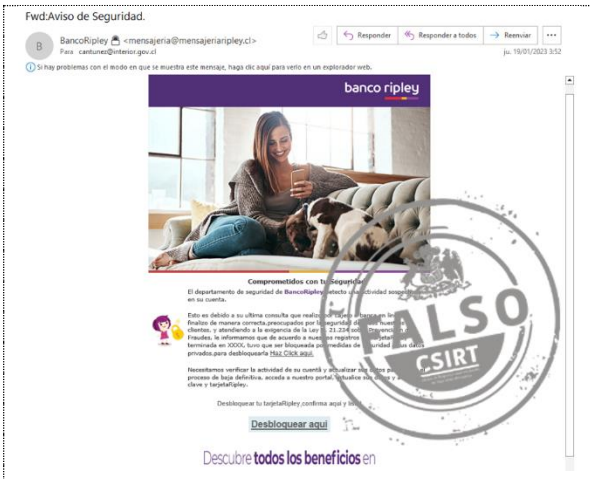
CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00718-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2023
Última revisión	18 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//ucmstudio[.]info/activacion/cuenta-aotq/	
URL sitio falso	
https[:]//smschilestado[.]info/1674045653/imagenes/_personas/home/default.asp	
Dirección IP	
[202.89.39.41]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00718-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00718-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00719-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	18 de enero de 2023
Última revisión	18 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//contalaserena[.]net/activacion/cuenta-kppf/	
https[:]//rplaycoin[.]top/1674064175/imagenes/_personas/home/default.asp	
URL sitio falso	
https[:]//web-bancoripley-cl.awadgallery.co[.]uk/1673526041/login	
Dirección IP	
[202.89.39.41]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00719-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00719-01.pdf	

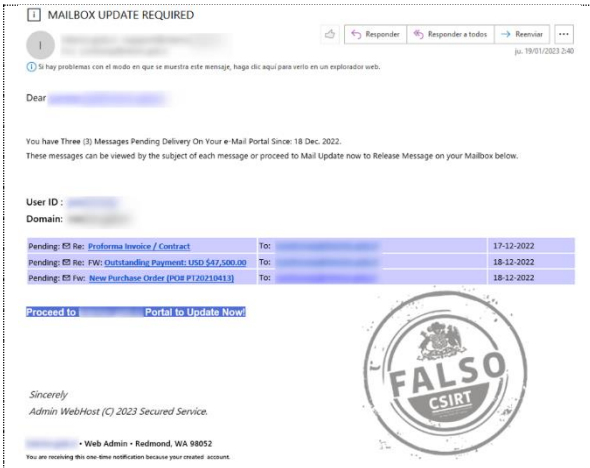


CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00720-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3iHv9uH?l=www.bancoripley.cl	
URL sitio falso	
https[:]//web.bancoripley.cl.bm-rentacar[.]com/1674069476/login	
Dirección IP	
[185.45.66.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00720-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00720-01.pdf	

CSIRT alerta de nueva campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH23-00721-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3BohsH2	
URL sitio falso	
https[:]//ingreso-banestado.web[.]app/WqTvcFQDmpdBcgzG/url?source=usg&pf_rd_r=fd6ni1ckga	
Dirección IP	
[199.36.158.100]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00721-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00721-01.pdf	



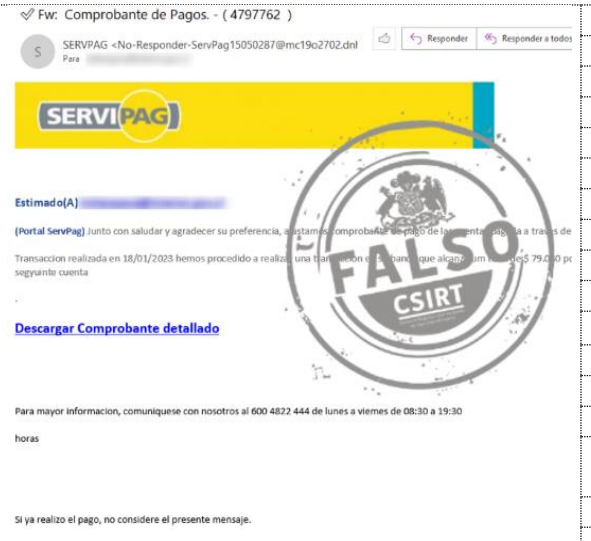
CSIRT alerta de nueva campaña de phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH23-00722-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero de 2023
Indicadores de compromiso	
URL redirección	
https[:]//bit[.]ly/3HfNI2m?l=www.bancoripley.cl	
URL sitio falso	
https://web.bancoripley.cl.bm-rentacar[.]com/1674241056/login	
Dirección IP	
[185.45.66.125]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00722-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00722-01.pdf	



CSIRT alerta de campaña de phishing que suplanta página de login de servicio de correo electrónico	
Alerta de seguridad cibernética	8FPH23-00723-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero de 2023
Indicadores de compromiso	
URL sitio falso	
https[:]//ipfs.io/ipfs/QmYaBZcHBefdcsjopwYGtWL7AewUkPPVdTgWXoFfwtQumE?filename=oglogz113_cham-e.html#test@csirt.gob.cl	
Dirección IP	
[209.94.90.1]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph23-00723-01/	
https://www.csirt.gob.cl/media/2023/01/8FPH23-00723-01.pdf	

3. Malware

CSIRT alerta de campaña de phishing con malware, que suplanta al SII	
Alerta de seguridad cibernética	2CMV23-00396-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2023
Última revisión	13 de enero de 2023
Indicadores de compromiso	
Asunto	
Atencion SII, Servicio de Impuestos internos	
Correo de Salida	
vendas@sallusmedical.com.br	
SHA256	
142972cf8f8f84f2fe9bc3f432b70d1c81f187291d1ae1f6903fb69abaee241d 964fbbc3b3a80e3e378e88f8c523d72e539ba06e46643ed212bc0609871fff4e	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00396-01/	
https://www.csirt.gob.cl/media/2023/01/2CMV23-00396-01.pdf	



CSIRT alerta de campaña de phishing con malware, que suplanta a Servipag	
Alerta de seguridad cibernética	2CMV23-00397-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de enero de 2023
Última revisión	19 de enero de 2023
Indicadores de compromiso	
Asunto	
✓✓ Fw: Comprobante de Pagos. - (4797762)	
Correo de Salida	
angel4.me@angel4.me	
SHA256	
6e6d0b550377356b6fa234f06a7f8348f48abec68b14396c713fd0aecb9cc075 d27fc5641cadee2fe89f1a23264ae10879cde5702397a4bb3c6ace6e583bc4b7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv23-00397-01/	
https://www.csirt.gob.cl/media/2023/01/2CMV23-00397-01.pdf	

4. Vulnerabilidades

CSIRT alerta de vulnerabilidades críticas en routers Cisco que no serán parchadas por la compañía	
Alerta de seguridad cibernética	9VSA23-00772-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de enero de 2023
Última revisión	16 de enero de 2023
CVE	
CVE-2023-20025 CVE-2023-20026	
Fabricantes	
Cisco	
Productos afectados	
Routers RV016 Multi-WAN VPN Routers RV042 Dual WAN VPN Routers RV042G Dual Gigabit WAN VPN Routers RV082 Dual WAN VPN	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00772-01/	
https://www.csirt.gob.cl/media/2022/12/9VSA22-00772-01.pdf	

CSIRT comparte vulnerabilidades en varios productos de Juniper Networks		
Alerta de seguridad cibernética	9VSA23-00773-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	17 de enero de 2023	
Última revisión	17 de enero de 2023	
CVE		
CVE-2019-17571	CVE-2021-46143	CVE-2020-14562
CVE-2020-8492	CVE-2020-36385	CVE-2022-21426
CVE-2020-14343	CVE-2021-37576	CVE-2021-35556
CVE-2020-12049	CVE-2020-0466	CVE-2021-35559
CVE-2020-14583	CVE-2022-0330	CVE-2021-35561
CVE-2020-14593	CVE-2020-12362	CVE-2021-35565
CVE-2020-27223	CVE-2021-22555	CVE-2021-35578
CVE-2021-21309	CVE-2021-29154	CVE-2021-35586
CVE-2022-22184	CVE-2021-33033	CVE-2022-21277
CVE-2007-6755	CVE-2021-33034	CVE-2022-21283
CVE-2019-1543	CVE-2021-3347	CVE-2022-21293
CVE-2019-1551	CVE-2021-33909	CVE-2022-21294
CVE-2023-22397	CVE-2021-3715	CVE-2022-21299
CVE-2020-28469	CVE-2021-4034	CVE-2022-21340
CVE-2021-23840	CVE-2021-4028	CVE-2022-21341
CVE-2021-3712	CVE-2021-27365	CVE-2022-21349
CVE-2021-3765	CVE-2022-0492	CVE-2022-21360
CVE-2023-22403	CVE-2021-22543	CVE-2022-21365

	CVE-2023-22407	CVE-2021-34798	CVE-2022-21366
	CVE-2023-22409	CVE-2020-27827	CVE-2020-14621
	CVE-2021-3156	CVE-2020-35498	CVE-2022-21434
	CVE-2020-14145	CVE-2018-25032	CVE-2022-21496
	CVE-2020-14871	CVE-2021-23840	CVE-2022-21549
	CVE-2023-22408	CVE-2021-27219	CVE-2021-35564
	CVE-2023-22406	CVE-2022-0778	CVE-2022-21291
	CVE-2023-22399	CVE-2022-38177	CVE-2022-21305
	CVE-2019-11287	CVE-2022-38178	CVE-2022-21540
	CVE-2023-22398	CVE-2022-21449	CVE-2020-14803
	CVE-2022-0778	CVE-2022-34169	CVE-2022-21282
	CVE-2023-22416	CVE-2022-21476	CVE-2022-21296
	CVE-2023-22401	CVE-2021-2388	CVE-2021-2163
	CVE-2023-22415	CVE-2020-14593	CVE-2019-20934
	CVE-2023-22412	CVE-2022-29154	CVE-2020-14556
	CVE-2023-22394	CVE-2021-3712	CVE-2020-27170
	CVE-2023-22393	CVE-2021-25217	CVE-2021-27363
	CVE-2023-22391	CVE-2020-26116	CVE-2021-2369
	CVE-2023-22414	CVE-2020-8648	CVE-2020-14792
	CVE-2023-22411	CVE-2021-27364	CVE-2020-14578
	CVE-2023-22396	CVE-2021-3752	CVE-2020-14579
	CVE-2023-22405	CVE-2021-32399	CVE-2021-2432
	CVE-2023-22400	CVE-2022-1729	CVE-2022-21443
	CVE-2023-22410	CVE-2021-4083	CVE-2020-14779
	CVE-2023-22404	CVE-2020-0465	CVE-2020-14573
	CVE-2023-22395	CVE-2021-35567	CVE-2020-14782
	CVE-2023-22417	CVE-2021-42739	CVE-2020-14797
	CVE-2023-22402	CVE-2020-26137	CVE-2022-21248
	CVE-2023-22413	CVE-2021-40085	CVE-2020-14577
	CVE-2022-22822	CVE-2020-24511	CVE-2020-14581
	CVE-2022-22823	CVE-2020-24513	CVE-2021-35603
	CVE-2022-22824	CVE-2021-0920	CVE-2020-14781
	CVE-2022-23852	CVE-2021-3573	CVE-2020-24512
	CVE-2022-25235	CVE-2021-23841	CVE-2020-14798
	CVE-2022-25236	CVE-2022-21541	CVE-2021-2341
	CVE-2022-25315	CVE-2021-2161	CVE-2020-14796
	CVE-2021-3177	CVE-2021-35550	CVE-2022-22942
	CVE-2021-39275	CVE-2020-11668	CVE-2022-29154
	CVE-2021-44790	CVE-2021-3564	CVE-2022-2526
	CVE-2022-22720	CVE-2020-12363	CVE-2022-21541
	CVE-2022-2526	CVE-2020-12364	CVE-2022-34169
	CVE-2021-26691	CVE-2021-29650	CVE-2022-21540
	CVE-2016-4658	CVE-2020-25704	CVE-2022-21624
	CVE-2021-40438	CVE-2020-36322	CVE-2022-21626
	CVE-2022-22825	CVE-2020-0543	CVE-2022-21628
	CVE-2022-22826	CVE-2020-0548	CVE-2022-21619
	CVE-2022-22827	CVE-2020-0549	CVE-2007-2285
	CVE-2021-3621	CVE-2020-8695	CVE-2018-8046
	CVE-2021-45960	CVE-2020-8696	CVE-2020-26137
	CVE-2022-1271	CVE-2020-8698	CVE-2021-3177
	CVE-2020-24489	CVE-2021-4155	CVE-2020-26116
	CVE-2021-30465	CVE-2022-21123	CVE-2022-1729
	CVE-2020-14583	CVE-2022-21125	CVE-2022-32250
	CVE-2021-42574	CVE-2022-21166	CVE-2022-1271
	CVE-2022-24903	CVE-2021-3504	

	Fabricantes
	Juniper Networks
	Productos afectados
	Contrail Cloud in release 13.7.0. Contrail Networking anteriores a la versión 2011. Contrail Networking versiones posteriores a R22.1 y anteriores a R22.3. Contrail Service Orchestration (CSO) anterior a 6.3.0. Junos OS 12.3 version 12.3R12-S19 and later versions. Junos OS 15.1 version 15.1R7-S10 and later versions. Junos OS 15.1 versions prior to 15.1R7-S12. Junos OS 17.3 version 17.3R3-S12 and later versions. Junos OS 18.4 version 18.4R3-S9 and later versions. Junos OS 19.1 version 19.1R3-S7 and later versions. Junos OS 19.1 versions prior to 19.1R3-S9. Junos OS 19.2 version 19.2R3-S3 and later versions. Junos OS 19.2 versions prior to 19.2R1-S9, 19.2R3-S5. Junos OS 19.3 version 19.3R2-S7, 19.3R3-S3 and later versions prior to 19.3R3-S7. Junos OS 19.3 versions prior to 19.3R3-S6. Junos OS 19.4 version 19.4R2-S7, 19.4R3-S5 and later versions prior to 19.4R3-10. Junos OS 19.4 versions prior to 19.4R2-S7, 19.4R3-S8. Junos OS 19.4 versions prior to 19.4R3-S9. Junos OS 20.1 version 20.1R1 and later versions. Junos OS 20.1 version 20.1R3-S1 and later versions. Junos OS 20.1 versions prior to 20.1R3-S4. Junos OS 20.2 version 20.2R3-S2 and later versions prior to 20.2R3-S6. Junos OS 20.2 versions prior to 20.2R3-S5. Junos OS 20.2 versions prior to 20.2R3-S5. Junos OS 20.3 version 20.3R3-S1 and later versions prior to 20.3R3-S6. Junos OS 20.3 versions prior to 20.3R3-S5. Junos OS 20.4 version 20.4R2-S2, 20.4R3 and later versions prior to 20.4R3-S5. Junos OS 20.4 versions prior to 20.4R3-S4. Junos OS 21.1 version 21.1R2 and later versions prior to 21.1R3-S4. Junos OS 21.1 versions prior to 21.1R1-S1, 21.1R2. Junos OS 21.1 versions prior to 21.1R3-S3. Junos OS 21.2 version 21.2R1-S1, 21.2R2 and later versions prior to 21.2R3-S3. Junos OS 21.2 versions prior to 21.2R3-S2. Junos OS 21.3 versions prior to 21.3R3-S1. Junos OS 21.3 versions prior to 21.3R3-S2. Junos OS 21.4 versions prior to 21.4R3. Junos OS 22.1 versions prior to 22.1R2. Junos OS 22.1 versions prior to 22.1R2-S1, 22.1R3. Junos OS 22.2 versions prior to 22.2R1-S2, 22.2R2. Junos OS 22.3 versions prior to 22.3R1-S1, 22.3R2. Junos OS All versions prior to 19.3R3-S7. Junos OS Evolved 21.1 versions prior to 21.1R2-EVO. Junos OS Evolved 21.1-EVO version 21.1R1-EVO and later versions. Junos OS Evolved 21.2-EVO versions prior to 21.2R3-S4-EVO. Junos OS Evolved 21.3 versions prior to 21.3R3-EVO. Junos OS Evolved 21.3-EVO version 21.3R1-EVO and later versions. Junos OS Evolved 21.4 versions prior to 21.4R2-EVO. Junos OS Evolved 21.4-EVO versions prior to 21.4R2-EVO. Junos OS Evolved 22.1 versions prior to 22.1R2-EVO. Junos OS Evolved 22.1-EVO versions prior to 22.1R3-EVO. Junos OS Evolved 22.2 versions prior to 22.2R1-S1-EVO, 22.2R2-EVO. Junos OS Evolved All versions prior to 20.4R3-S3-EVO.

	Junos OS Evolved All versions prior to 20.4R3-S4. Junos OS Evolved on PTX10003 21.3 versions prior to 21.3R3-S1-EVO. Junos OS Evolved on PTX10003 All versions prior to 20.4R3-S4-EVO. Junos OS Evolved on PTX1000321.4 versions prior to 21.4R2-S2-EVO, 21.4R3-VO. Junos OS Evolved on PTX1000322.1 versions prior to 22.1R1-S2-EVO, 22.1R2-VO. Junos OS Evolved on PTX1000322.2 versions prior to 22.2R2-EVO. Junos OS Evolved versión 22.3R1-EVO. Junos OS Evolved19.3 versions prior to 19.3R3-EVO. Junos OS Evolved19.4 versions prior to 19.4R3-EVO. Junos OS Evolved20.1 versions prior to 20.1R3-EVO. Junos OS Evolved20.2 versions prior to 20.2R2-EVO. Junos OS Evolved21.1 versions prior to 21.1R2-EVO. Junos OS Evolved21.2 version 21.2R1 and later versions. Junos OS Evolved21.3 versions prior to 21.3R2-EVO. Junos OS Evolved21.3-EVO version 21.3R3-EVO and later versions. Junos OS Evolved21.4 versions prior to 21.4R2-S1-EVO, 21.4R3-EVO. Junos OS Evolved21.4-EVO version 21.4R1-S2-EVO, 21.4R2-EVO and later prior to 21.4R2-S1-EVO. Junos OS Evolved21.4-EVO versions prior to 21.4R2-S2-EVO, 21.4R3-EVO. Junos OS Evolved22.1 versions prior to 22.1R2-EVO. Junos OS Evolved22.1-EVO version 22.1R2-EVO and later versions prior to 22.1R3-EVO. Junos OS Evolved22.1-EVO versions prior to 22.1R1-S2-EVO, 22.1R2-EVO. Junos OS Evolved22.2-EVO versions prior to 22.2R1-S1-EVO, 22.2R2-EVO. Junos OS Evolved22.2-EVO versions prior to 22.2R1-S1-EVO, 22.2R2-EVO. Junos OS EvolvedAll versions prior to 19.2R3-EVO. Junos OS EvolvedAll versions prior to 20.4R2-EVO. Junos OS EvolvedAll versions prior to 20.4R3-S4-EVO. Junos OS on ACX2K Series 20.3 versions prior to 20.3R3-S6. Junos OS on ACX2K Series 20.4 versions prior to 20.4R3-S4. Junos OS on ACX2K Series 21.2 versions prior to 21.2R3-S3. Junos OS on ACX2K Series All 20.2 versions. Junos OS on ACX2K Series All 21.1 versions. Junos OS on ACX2K Series All versions prior to 19.4R3-S9. Junos OS on MX Series 20.3 version 20.3R1 and later versions. Junos OS on MX Series All versions prior to 20.2R3-S5. Junos OS on MX Series and SRX Series 20.2 versions prior to 20.2R3-S6. Junos OS on MX Series and SRX Series 20.3 versions prior to 20.3R3-S6. Junos OS on MX Series and SRX Series 20.4 versions prior to 20.4R3-S5. Junos OS on MX Series and SRX Series 21.1 versions prior to 21.1R3-S4. Junos OS on MX Series and SRX Series 21.2 versions prior to 21.2R3-S2. Junos OS on MX Series and SRX Series 21.2 versions prior to 21.2R3-S3. Junos OS on MX Series and SRX Series 21.3 versions prior to 21.3R3-S1. Junos OS on MX Series and SRX Series 21.4 versions prior to 21.4R3. Junos OS on MX Series and SRX Series 22.1 versions prior to 22.1R1-S2, 22.1R2. Junos OS on MX Series and SRX Series 22.1 versions prior to 22.1R2-S1, 22.1R3. Junos OS on MX Series and SRX Series 22.2 versions prior to 22.2R1-S1, 22.2R2. Junos OS on MX Series and SRX Series 22.2 versions prior to 22.2R1-S2, 22.2R2. Junos OS on MX Series and SRX Series All versions prior to 19.4R3-S10. Junos OS on MX Series20.1 version 20.1R3-S5 and later versions. Junos OS on MX Series20.2 versions prior to 20.2R3-S5. Junos OS on MX Series20.3 versions prior to 20.3R3-S5. Junos OS on MX Series20.4 versions prior to 20.4R3-S4. Junos OS on MX Series21.1 versions prior to 21.1R3-S3. Junos OS on MX Series21.2 versions prior to 21.2R3-S1.

	Junos OS on MX Series21.3 versions prior to 21.3R3. Junos OS on MX Series21.4 versions prior to 21.4R2-S1, 21.4R3. Junos OS on MX Series22.1 versions prior to 22.1R2. Junos OS on MX SeriesAll versions prior to 19.4R3-S9. Junos OS on QFX10K Series 20.2 versions prior to 20.2R3-S6. Junos OS on QFX10K Series 20.3 versions prior to 20.3R3-S6. Junos OS on QFX10K Series 20.4 versions prior to 20.4R3-S5. Junos OS on QFX10K Series 21.1 versions prior to 21.1R3-S4. Junos OS on QFX10K Series 21.2 versions prior to 21.2R3-S3. Junos OS on QFX10K Series 21.3 versions prior to 21.3R3-S2. Junos OS on QFX10K Series 21.4 versions prior to 21.4R2-S2, 21.4R3. Junos OS on QFX10K Series 22.1 versions prior to 22.1R2. Junos OS on QFX10K Series 22.2 versions prior to 22.2R1-S2, 22.2R2. Junos OS on QFX10K Series All versions prior to 19.4R3-S9. Junos OS on QFX10K Series: Junos OS on QFX5k Series, EX46xx Series Junos OS on QFX5k Series, EX46xx Series 20.3 versions prior to 20.3R3-S5. Junos OS on QFX5k Series, EX46xx Series 20.4 versions prior to 20.4R3-S4. Junos OS on QFX5k Series, EX46xx Series 21.1 versions prior to 21.1R3-S3. Junos OS on QFX5k Series, EX46xx Series 21.2 versions prior to 21.2R3-S1. Junos OS on QFX5k Series, EX46xx Series 21.3 versions prior to 21.3R3 on. Junos OS on QFX5k Series, EX46xx Series 21.4 versions prior to 21.4R3 on. Junos OS on QFX5k Series, EX46xx Series 22.1 versions prior to 22.1R2 on. Junos OS on QFX5k Series, EX46xx Series All versions prior to 20.2R3-S5. Junos OS on SRX 5000 Series 20.4 versions prior to 20.4R3-S5. Junos OS on SRX 5000 Series 21.1 versions prior to 21.1R3-S4. Junos OS on SRX 5000 Series 21.2 versions prior to 21.2R3-S3. Junos OS on SRX 5000 Series 21.3 versions prior to 21.3R3-S3. Junos OS on SRX 5000 Series 21.4 versions prior to 21.4R3-S2. Junos OS on SRX 5000 Series 22.1 versions prior to 22.1R2-S2, 22.1R3. Junos OS on SRX 5000 Series 22.2 versions prior to 22.2R3. Junos OS on SRX 5000 Series 22.3 versions prior to 22.3R1-S1, 22.3R2. Junos OS on SRX Series 19.2 versions prior to 19.2R3-S6. Junos OS on SRX Series 19.3 versions prior to 19.3R3-S6. Junos OS on SRX Series 19.4 versions prior to 19.4R2-S8, 19.4R3-S10. Junos OS on SRX Series 19.4 versions prior to 19.4R3-S9. Junos OS on SRX Series 20.2 versions prior to 20.2R3-S5. Junos OS on SRX Series 20.2 versions prior to 20.2R3-S6. Junos OS on SRX Series 20.3 versions prior to 20.3R3-S4. Junos OS on SRX Series 20.3 versions prior to 20.3R3-S5. Junos OS on SRX Series 20.4 versions prior to 20.4R3-S3. Junos OS on SRX Series 20.4 versions prior to 20.4R3-S5. Junos OS on SRX Series 21.1 versions prior to 21.1R3. Junos OS on SRX Series 21.1 versions prior to 21.1R3-S4. Junos OS on SRX Series 21.2 versions prior to 21.2R3. Junos OS on SRX Series 21.3 versions prior to 21.3R2. Junos OS on SRX Series 21.3 versions prior to 21.3R3. Junos OS on SRX Series 21.4 versions prior to 21.4R2. Junos OS on SRX Series All versions prior to 19.3R3-S7. Junos OS on SRX Series and on MX Series 19.4 versions prior to 19.4R2-S8, 19.4R3-S10. Junos OS on SRX Series and on MX Series 20.1 versions 20.1R1 and later versions. Junos OS on SRX Series and on MX Series 20.2 versions prior to 20.2R3-S6. Junos OS on SRX Series and on MX Series 20.3 versions prior to 20.3R3-S6. Junos OS on SRX Series and on MX Series 20.4 versions prior to 20.4R3-S5.

	Junos OS on SRX Series and on MX Series 21.1 versions prior to 21.1R3-S5. Junos OS on SRX Series and on MX Series 21.2 versions prior to 21.2R3-S1. Junos OS on SRX Series and on MX Series 21.3 versions prior to 21.3R3. Junos OS on SRX Series and on MX Series 21.4 versions prior to 21.4R2-S2, 21.4R3. Junos OS on SRX Series and on MX Series 22.1 versions prior to 22.1R1-S2, 22.1R2, 22.1R3-S1. Junos OS on SRX Series and on MX Series All versions prior to 19.3R3-S7. Junos OS on SRX Series, and MX Series with SPC3 19.4 versions prior to 19.4R3-9. Junos OS on SRX Series, and MX Series with SPC3 20.1 version 20.1R1 and later versions. Junos OS on SRX Series, and MX Series with SPC3 All versions prior to 19.3R3-S7. Junos OS on SRX Series, and MX Series with SPC3 All versions prior to 19.4R3-S10. Junos OS on SRX Series, and MX Series with SPC320.2 versions prior to 20.2R3-S5. Junos OS on SRX Series, and MX Series with SPC320.2 versions prior to 20.2R3-S6. Junos OS on SRX Series, and MX Series with SPC320.3 versions prior to 20.3R3-S5. Junos OS on SRX Series, and MX Series with SPC320.3 versions prior to 20.3R3-S6. Junos OS on SRX Series, and MX Series with SPC320.4 versions prior to 20.4R3-S4. Junos OS on SRX Series, and MX Series with SPC320.4 versions prior to 20.4R3-S5. Junos OS on SRX Series, and MX Series with SPC321.1 versions prior to 21.1R3-S3. Junos OS on SRX Series, and MX Series with SPC321.1 versions prior to 21.1R3-S4. Junos OS on SRX Series, and MX Series with SPC321.2 versions prior to 21.2R3-S2. Junos OS on SRX Series, and MX Series with SPC321.2 versions prior to 21.2R3-S3. Junos OS on SRX Series, and MX Series with SPC321.3 versions prior to 21.3R3-S1. Junos OS on SRX Series, and MX Series with SPC321.3 versions prior to 21.3R3-S3. Junos OS on SRX Series, and MX Series with SPC321.4 versions prior to 21.4R2-S1, 21.4R3. Junos OS on SRX Series, and MX Series with SPC321.4 versions prior to 21.4R3-S1. Junos OS on SRX Series, and MX Series with SPC322.1 versions prior to 22.1R1-S2, 22.1R2. Junos OS on SRX Series, and MX Series with SPC322.1 versions prior to 22.1R2-S2, 22.1R3. Junos OS on SRX Series, and MX Series with SPC322.2 versions prior to 22.2R2. Junos OS PTX Series and QFX10000 Series20.2 versions prior to 20.2R3-S6. Junos OS PTX Series and QFX10000 Series20.3 versions prior to 20.3R3-S6. Junos OS PTX Series and QFX10000 Series20.4 versions prior to 20.4R3-S4. Junos OS PTX Series and QFX10000 Series21.1 versions prior to 21.1R3-S3. Junos OS PTX Series and QFX10000 Series21.2 versions prior to 21.2R3-S1. Junos OS PTX Series and QFX10000 Series21.3 versions prior to 21.3R3. Junos OS PTX Series and QFX10000 Series21.4 versions prior to 21.4R3. Junos OS PTX Series and QFX10000 Series22.1 versions prior to 22.1R2. Junos OS PTX Series and QFX10000 Series22.2 versions prior to 22.2R2. Junos OS versión 22.3R1. Junos OS:20.4 versions prior to 20.4R3-S4. Junos OS:21.1 versions prior to 21.1R3-S3. Junos OS:21.2 versions prior to 21.2R3-S1. Junos OS:21.3 versions prior to 21.3R3. Junos OS:21.4 versions prior to 21.4R3. Junos OS:22.1 versions prior to 22.1R2. Junos OS All versions prior to 20.2R3-S7. Junos OS19.1 versions prior to 19.1R3-S2. Junos OS19.2 version 19.2R1 and later versions. Junos OS19.2 versions prior to 19.2R3. Junos OS19.3 versions prior to 19.3R3. Junos OS19.3 versions prior to 19.3R3-S6.

	Junos OS19.4 versions prior to 19.4R2-S7, 19.4R3-S9. Junos OS19.4 versions prior to 19.4R2-S8, 19.4R3-S9. Junos OS19.4 versions prior to 19.4R3. Junos OS20.1 versions prior to 20.1R2. Junos OS20.1 versions prior to 20.1R3-S4. Junos OS20.2 versions prior to 20.2R2. Junos OS20.2 versions prior to 20.2R3-S5. Junos OS20.2 versions prior to 20.2R3-S5. Junos OS20.3 versions prior to 20.3R3-S4. Junos OS20.3 versions prior to 20.3R3-S5. Junos OS20.4 versions prior to 20.4R3-S4. Junos OS20.4 versions prior to 20.4R3-S4. Junos OS21.1 versions prior to 21.1R3-S3. Junos OS21.1 versions prior to 21.1R3-S3. Junos OS21.1 versions prior to 21.1R3-S4. Junos OS21.2 versions prior to 21.2R3-S1. Junos OS21.2 versions prior to 21.2R3-S2. Junos OS21.2 versions prior to 21.2R3-S3. Junos OS21.3 versions prior to 21.3R3-S1. Junos OS21.3 versions prior to 21.3R3-S1. Junos OS21.3 versions prior to 21.3R3-S2. Junos OS21.4 versions prior to 21.4R2. Junos OS21.4 versions prior to 21.4R2-S1, 21.4R3. Junos OS21.4 versions prior to 21.4R2-S2, 21.4R3. Junos OS22.1 version 22.1R2 and later versions. Junos OS22.1 versions prior to 22.1R1-S2, 22.1R2. Junos OS22.1 versions prior to 22.1R2. Junos OS22.1 versions prior to 22.1R2. Junos OS22.1 versions prior to 22.1R3. Junos OS22.2 versions prior to 22.2R1-S1, 22.2R2. Junos OS22.2 versions prior to 22.2R2. Junos OSAll versions prior to 18.4R2-S7. Junos OSAll versions prior to 19.1R3-S9. Junos OSAll versions prior to 19.3R3-S7. Junos Space versions prior to 22.3R1. NorthStar Controller versions prior to 6.2.3.
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00773-01/
	https://www.csirt.gob.cl/media/2023/01/9VSA23-00773-01.pdf

CSIRT comparte informe de vulnerabilidades parchadas por Oracle en su Critical Patch Update de Enero 2023	
Alerta de seguridad cibernética	9VSA23-00774-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2023
Última revisión	11 de enero de 2023

CVE

CVE-2018-1273	CVE-2022-25857	CVE-2023-21842
CVE-2018-25032	CVE-2022-26336	CVE-2023-21843
CVE-2018-7489	CVE-2022-27404	CVE-2023-21844
CVE-2019-12415	CVE-2022-27782	CVE-2023-21845
CVE-2019-17571	CVE-2022-29824	CVE-2023-21846
CVE-2019-7317	CVE-2022-30126	CVE-2023-21847
CVE-2020-10683	CVE-2022-3028	CVE-2023-21848
CVE-2020-10693	CVE-2022-30293	CVE-2023-21849
CVE-2020-10735	CVE-2022-31129	CVE-2023-21850
CVE-2020-11979	CVE-2022-31629	CVE-2023-21851
CVE-2020-11987	CVE-2022-31692	CVE-2023-21852
CVE-2020-13956	CVE-2022-3171	CVE-2023-21853
CVE-2020-16156	CVE-2022-31813	CVE-2023-21854
CVE-2020-27844	CVE-2022-32212	CVE-2023-21855
CVE-2020-36242	CVE-2022-32221	CVE-2023-21856
CVE-2020-36518	CVE-2022-33980	CVE-2023-21857
CVE-2021-23358	CVE-2022-34169	CVE-2023-21858
CVE-2021-2351	CVE-2022-34305	CVE-2023-21859
CVE-2021-29425	CVE-2022-34917	CVE-2023-21860
CVE-2021-31805	CVE-2022-3510	CVE-2023-21861
CVE-2021-31812	CVE-2022-35737	CVE-2023-21862
CVE-2021-36090	CVE-2022-36033	CVE-2023-21863
CVE-2021-36483	CVE-2022-36055	CVE-2023-21864
CVE-2021-36770	CVE-2022-37434	CVE-2023-21865
CVE-2021-3737	CVE-2022-37454	CVE-2023-21866
CVE-2021-37533	CVE-2022-38752	CVE-2023-21867
CVE-2021-3918	CVE-2022-39271	CVE-2023-21868
CVE-2021-40528	CVE-2022-39429	CVE-2023-21869
CVE-2021-41184	CVE-2022-40146	CVE-2023-21870
CVE-2021-41411	CVE-2022-40149	CVE-2023-21871
CVE-2021-42717	CVE-2022-40150	CVE-2023-21872
CVE-2021-43797	CVE-2022-40153	CVE-2023-21873
CVE-2021-44832	CVE-2022-40304	CVE-2023-21874
CVE-2021-45105	CVE-2022-40664	CVE-2023-21875
CVE-2022-0084	CVE-2022-4147	CVE-2023-21876
CVE-2022-0492	CVE-2022-41720	CVE-2023-21877
CVE-2022-0934	CVE-2022-41881	CVE-2023-21878
CVE-2022-1122	CVE-2022-42003	CVE-2023-21879
CVE-2022-1304	CVE-2022-42252	CVE-2023-21880
CVE-2022-1319	CVE-2022-42889	CVE-2023-21881
CVE-2022-1941	CVE-2022-42915	CVE-2023-21882
CVE-2022-2048	CVE-2022-42920	CVE-2023-21883
CVE-2022-2053	CVE-2022-43403	CVE-2023-21884
CVE-2022-21824	CVE-2022-43548	CVE-2023-21885
CVE-2022-2274	CVE-2022-43680	CVE-2023-21886

CVE-2022-22965	CVE-2022-45047	CVE-2023-21887
CVE-2022-22970	CVE-2023-21824	CVE-2023-21888
CVE-2022-22971	CVE-2023-21825	CVE-2023-21889
CVE-2022-22978	CVE-2023-21826	CVE-2023-21890
CVE-2022-23219	CVE-2023-21827	CVE-2023-21891
CVE-2022-23221	CVE-2023-21828	CVE-2023-21892
CVE-2022-23305	CVE-2023-21829	CVE-2023-21893
CVE-2022-23437	CVE-2023-21830	CVE-2023-21894
CVE-2022-23457	CVE-2023-21831	CVE-2023-21898
CVE-2022-24329	CVE-2023-21832	CVE-2023-21899
CVE-2022-24407	CVE-2023-21834	CVE-2023-21900
CVE-2022-24823	CVE-2023-21835	CVE-2021-21708
CVE-2022-24839	CVE-2023-21836	CVE-2022-2047
CVE-2022-24903	CVE-2023-21837	CVE-2022-21597
CVE-2022-2509	CVE-2023-21838	CVE-2022-2191
CVE-2022-25236	CVE-2023-21839	CVE-2022-22950
CVE-2022-2526	CVE-2023-21840	CVE-2022-38749
CVE-2022-25315	CVE-2023-21841	CVE-2022-38750
CVE-2022-25647	CVE-2022-42004	CVE-2022-38751

Fabricantes

Adobe

Productos afectados

Enterprise Manager Base Platform13.4.0.0, 13.5.0.0
Enterprise Manager Ops Center12.4.0.0
Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S ServersPrior to XCP2411, prior to XCP3111, prior to XCP4011
GoldenGate Stream AnalyticsPrior to 19.1.0.0.8
Java VM19c, 21c
JD Edwards EnterpriseOne OrchestratorPrior to 9.2.7.2
JD Edwards EnterpriseOne ToolsPrior to 9.2.7.2
Management Cloud Engine22.1.0.0.0
Middleware Common Libraries and Tools12.2.1.4.0, 14.1.1.0.0
MySQL Cluster7.4.38 and prior,7.5.28 and prior,7.6.24 and prior, 8.0.31 and prior
MySQL Connectors8.0.31 and prior
MySQL Enterprise Monitor8.0.32 and prior
MySQL Server5.7.40 and prior
MySQL Server5.7.40 and prior, 8.0.31 and prior
MySQL Server8.0.28 and prior
MySQL Server8.0.29 and prior
MySQL Server8.0.30 and prior
MySQL Server8.0.31 and prior
MySQL Shell8.0.31 and prior
MySQL Workbench8.0.31 and prior
Oracle Access Manager12.2.1.4.0
Oracle Agile PLM9.3.6
Oracle Applications DBA 12.2.3-12.2.12
Oracle AutoVuePrior to 21.0.2.0
Oracle AutoVuePrior to 21.0.2.6
Oracle Banking Enterprise Default Management 2.6.2
Oracle Banking Enterprise Default Management 2.7.0
Oracle Banking Enterprise Default Management 2.7.1, 2.12.0
Oracle Banking Loans Servicing 2.8.0, 2.12.0
Oracle Banking Party Management 2.7.0
Oracle Banking Platform2.6.2, 2.7.1, 2.9.0, 2.12.0
Oracle BI Publisher5.9.0.0.0, 6.4.0.0.0, 12.2.1.4.0

	Oracle Business Intelligence Enterprise Edition5.9.0.0.0, 6.4.0.0.0 Oracle Coherence12.2.1.3.0, 12.2.1.4.0 Oracle Coherence14.1.1.0.0 Oracle Collaborative Planning12.2.3-12.2.12 Oracle Commerce Guided Search11.3.2 Oracle Communications Billing and Revenue Management12.0.0.4.0-12.0.0.7.0 Oracle Communications BRM – Elastic Charging Engine12.0.0.3.0-12.0.0.7.0 Oracle Communications Calendar Server8.0.0.6.0 Oracle Communications Cloud Native Core Automated Test Suite22.2.2, 22.3.1, 22.4.0 Oracle Communications Cloud Native Core Binding Support Function 22.1.0, 22.2.0 Oracle Communications Cloud Native Core Binding Support Function 22.1.1 Oracle Communications Cloud Native Core Binding Support Function 22.2.0 Oracle Communications Cloud Native Core Binding Support Function 22.2.0, 22.2.2, 22.3.1 Oracle Communications Cloud Native Core Binding Support Function 22.2.1 Oracle Communications Cloud Native Core Binding Support Function 22.2.2 Oracle Communications Cloud Native Core Binding Support Function 22.2.4 Oracle Communications Cloud Native Core Binding Support Function 22.3.0 Oracle Communications Cloud Native Core Binding Support Function 22.3.0-22.4.0 Oracle Communications Cloud Native Core Binding Support Function 22.3.2, 22.2.0 Oracle Communications Cloud Native Core Console 22.3.0 Oracle Communications Cloud Native Core Console 22.3.0, 22.4.0 Oracle Communications Cloud Native Core Network Data Analytics Function22.0.0.0.0 Oracle Communications Cloud Native Core Network Exposure Function 22.3.1 Oracle Communications Cloud Native Core Network Exposure Function 22.3.1, 22.4.0 Oracle Communications Cloud Native Core Network Function Cloud Native Environment22.3.0 Oracle Communications Cloud Native Core Network Repository Function 22.3.0 Oracle Communications Cloud Native Core Network Repository Function 22.3.2 Oracle Communications Cloud Native Core Network Slice Selection Function22.3.1 Oracle Communications Cloud Native Core Network Slice Selection Function22.3.1, 22.4.1 Oracle Communications Cloud Native Core Policy1.11.0 Oracle Communications Cloud Native Core Policy22.3.0 Oracle Communications Cloud Native Core Policy22.3.0, 22.4.0 Oracle Communications Cloud Native Core Security Edge Protection Proxy 22.3.1 Oracle Communications Cloud Native Core Security Edge Protection Proxy 22.4.0, 22.3.1 Oracle Communications Cloud Native Core Unified Data Repository 22.2.2, 22.3.3 Oracle Communications Cloud Native Core Unified Data Repository 22.3.3 Oracle Communications Cloud Native Core Unified Data Repository 22.3.3, 22.4.0 Oracle Communications Cloud Native Core Unified Data Repository 22.3.4, 22.2.3 Oracle Communications Contacts Server8.0.0.7.0 Oracle Communications Converged Application Server7.1.0, 8.0.0 Oracle Communications Convergence3.0.3.1.0 Oracle Communications Design Studio7.4.2 Oracle Communications Diameter Intelligence Hub8.2.3.0 Oracle Communications Diameter Signaling Router8.6.0.0

	Oracle Communications Elastic Charging Engine 12.0.0.3.0-12.0.0.7.0 Oracle Communications Elastic Charging Engine 12.0.0.5.0-12.0.0.7.0 Oracle Communications Instant Messaging Server 10.0.1.6.0 Oracle Communications Messaging Server 8.1.0.20.0 Oracle Communications MetaSolv Solution 6.3.1 Oracle Communications Order and Service Management 7.4.0 Oracle Communications Performance Intelligence Center (PIC) Software 10.4.0.4.1 Oracle Communications Pricing Design Center 12.0.0.5.0-12.0.0.7.0 Oracle Communications Unified Assurance 5.5.0-5.5.9 Oracle Communications Unified Assurance 5.5.0-5.5.9, 6.0.0-6.0.1 Oracle Communications Unified Inventory Management 7.4.0, 7.4.1, 7.4.2 Oracle Communications Unified Inventory Management 7.4.0, 7.4.1, 7.4.2, 7.5.0 Oracle Communications Unified Inventory Management 7.4.0-7.4.2, 7.5.0 Oracle Communications Unified Inventory Management 7.5.0 Oracle Data Provider for .NET 19c, 21c Oracle Database – Machine Learning for Python (Python) 21c Oracle Database – Workload Manager (jackson-databind) 21c Oracle Database (Python) 21c Oracle Database (zlib) 19c, 21c Oracle Database Data Redaction 19c, 21c Oracle Database Fleet Patching (jackson-databind) 21c Oracle Database RDBMS Security 19c, 21c Oracle Demantra Demand Management 12.1, 12.2 Oracle Demantra Demand Management 12.2.7, 12.2.8, 12.2.9, 12.2.10, 12.2.11, 12.2.12 Oracle Documaker 12.4.0-12.7.0 Oracle Essbase 21.4 Oracle Financial Services Crime and Compliance Management Studio 8.0.8.3.1 Oracle Fusion Middleware MapViewer 12.2.1.4.0 Oracle Global Lifecycle Management NextGen OUI FrameworkPrior to 13.9.4.2.11 Oracle GraalVM Enterprise EditionOracle GraalVM Enterprise Edition: 20.3.8, 21.3.4, 22.3.0 Oracle HCM Common Architecture 12.2.3-12.2.12 Oracle Health Sciences Empirica Signal 9.1.0.52, 9.2.0.52 Oracle Healthcare Data Repository 8.1.0.0-8.1.3.1 Oracle Healthcare Translational Research 4.1.0.0-4.1.1.1 Oracle Hospitality Cruise Shipboard Property Management System 20.2.2 Oracle Hospitality Gift and Loyalty 9.1.0 Oracle Hospitality Labor Management 9.1.0 Oracle Hospitality Reporting and Analytics 9.1.0 Oracle Hospitality Simphony 18.2.11, 19.3.4 Oracle HTTP Server 12.2.1.4.0 Oracle Hyperion Infrastructure Technology 11.2.10 Oracle iSetup 12.2.3-12.2.12 Oracle iSupplier Portal 12.2.6-12.2.8 Oracle Java SE, Oracle GraalVM Enterprise EditionOracle Java SE: 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4, 22.3.0 Oracle Java SE, Oracle GraalVM Enterprise EditionOracle Java SE: 8u351, 8u351-perf, 11.0.17, 17.0.5, 19.0.1; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4, 22.3.0 Oracle Java SE, Oracle GraalVM Enterprise Edition Oracle Java SE: 8u351, 8u351-perf; Oracle GraalVM Enterprise Edition: 20.3.8, 21.3.4 Oracle Learning Management 12.2.3-12.2.12 Oracle Marketing 12.2.3-12.2.12

	Oracle Middleware Common Libraries and Tools 12.2.1.4.0 Oracle Mobile Field Service 12.2.3-12.2.12 Oracle Outside In Technology 8.5.6 Oracle Retail Service Backbone 14.1.3.2, 15.0.3.1, 16.0.3 Oracle Sales for Handhelds 12.2.3-12.2.12 Oracle Sales Offline 12.2.3-12.2.12 Oracle Self-Service Human Resources 12.2.3-12.2.12 Oracle Solaris10, 11 Oracle Stream Analytics Prior to 19.1.0.0.8 Oracle TimesTen In-Memory Database Prior to 11.2.2.8.65 Oracle Utilities Framework 4.3.0.5.0, 4.3.0.6.0, 4.4.0.0.0, 4.4.0.2.0, 4.4.0.3.0, 4.5.0.0.0 Oracle Utilities Framework 4.4.0.3.0, 4.5.0.0.0 Oracle Utilities Network Management System 2.3.0.2, 2.4.0.1, 2.5.0.0, 2.5.0.1, 2.5.0.2 Oracle Utilities Network Management System 2.3.0.2, 2.4.0.1, 2.5.0.0-2.5.0.2 Oracle Utilities Network Management System 2.5.0.1, 2.5.0.2 Oracle VM VirtualBox Prior to 6.1.42, prior to 7.0.6 Oracle Web Applications Desktop Integrator 12.2.3-12.2.12 Oracle Web Services Manager 12.2.1.4.0 Oracle WebCenter Content 12.2.1.4.0 Oracle WebCenter Sites 12.2.1.4.0 Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0 Oracle WebLogic Server 12.2.1.3.0, 12.2.1.4.0, 14.1.1.0.0 Oracle WebLogic Server 14.1.1.0.0 OSS Support Tools 2.12.43 OSS Support Tools 22.2.22.4.5 OSS Support Tools 22.4.22.10.18 PeopleSoft Enterprise CC Common Application Objects 9.2 PeopleSoft Enterprise CS Academic Advisement 9.2 PeopleSoft Enterprise PeopleTools 8.58 PeopleSoft Enterprise PeopleTools 8.58, 8.59, 8.60 PeopleSoft Enterprise PeopleTools 8.59, 8.60 PeopleSoft Enterprise PeopleTools 8.60 Primavera Gateway 18.8.0-18.8.15, 19.12.0-19.12.15, 20.12.0-20.12.10, 21.12.0-21.12.8 Primavera Unifier 18.8, 19.12, 20.12, 21.12, 22.12 ProductSupported Versions Affected Siebel Apps – Marketing22.10 and prior Siebel CRM22.10 and prior
	Enlaces para revisar el informe:
	https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00774-01/
	https://www.csirt.gob.cl/media/2023/01/9VSA23-00774-01.pdf

CSIRT comparte vulnerabilidades parchadas en Mozilla Firefox y Firefox ESR		
Alerta de seguridad cibernética	9VSA23-00775-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Crítico	
TLP	Blanco	
Fecha de lanzamiento original	18 de enero de 2023	
Última revisión	18 de enero de 2023	
CVE		
CVE-2023-23599 CVE-2023-23601 CVE-2023-23603	CVE-2023-23602 CVE-2023-23605 CVE-2022-46871	CVE-2022-46877 CVE-2023-23598
Fabricantes		
Mozilla		
Productos afectados		
Versiones anteriores a Firefox ESR 102.7 Versiones anteriores a Firefox 109		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa23-00775-01/		
https://www.csirt.gob.cl/media/2023/01/9VSA23-00775-01.pdf		

5. Concientización

Ciberconsejos | Cómo activar la verificación de dos pasos en TikTok

TikTok es una de las aplicaciones más populares el orbe, siendo usada principalmente por niños y jóvenes. Y como en cualquier otra aplicación en la que debamos registrarnos como usuarios, nuestra cuenta siempre estará en riesgo de poder ser secuestrada o robada por actores maliciosos.

Por lo anterior es que les entregamos los siguientes ciberconsejos, que explican cómo activar la verificación en dos pasos en TikTok. Pueden encontrar la campaña y todas las anteriores que hemos hecho, en nuestro sitio web oficial: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-verificacion-tiktok

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.

- Víctor José Palomo Arredondo
- Gabriel Zamora Vargas
- Diego González
- Moisés Brito López
- Matías Nicolás Enrique Zamorano Pino
- Jerson Valenzuela Campusano
- Gabriel Vigoroux Pereira
- Rodrigo Álvaro Vallejos Maureira
- Eduardo Andrés Riveros Roca
- Jenny Garrido Escobar

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.01.20 17:32:34 -03'00'