Ministerio del Interior y Seguridad Pública

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

14-01-2022 | Año 4 | N°132

Boletín de Seguridad Cibernética

Semana del 7 al 13 de enero de 2022

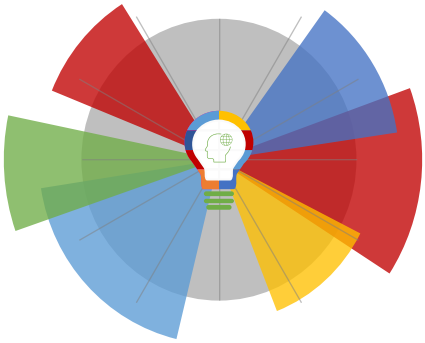
La semana en cifras

Parches

184

para vulnerabilidades

Las mitigaciones son útiles en productos de Microsoft, Mozilla, SAP, Adobe y Google Android



Se advirtieron

9

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

5

Informadas

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

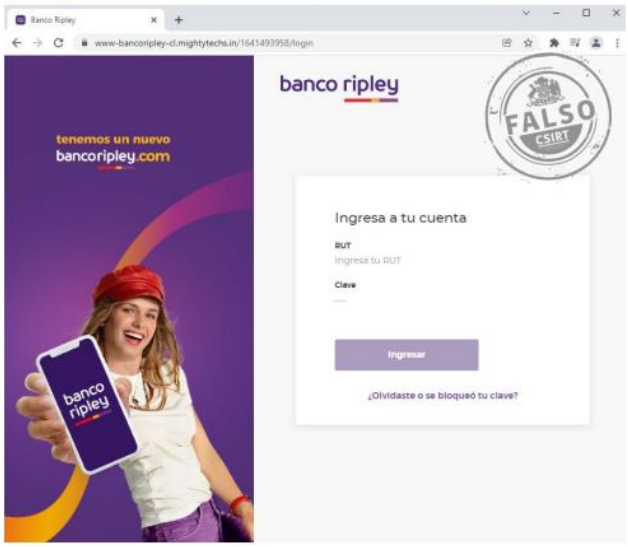
*Los datos recopilados corresponden a información publicada en diferentes secciones del sitio web https://www.csirt.gob.cl.

Contenido

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Sitios fraudulentos

Imagen del sitio



CSIRT informa sitio que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FFR21-01047-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	7 de enero de 2022
Última revisión	7 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://www-bancoripley-cl.mightytechs[.]in/1641489095/login	
URL redirección	
https://bit[.]ly/3zbRsMK?|=www.bancoripley.cl	
http://stz-fmba[.]ru/wp-includes/certificates/enviar02.php?l=509398429	
https://sspmprimaryschool[.]com/activacion/cuenta-pqdw/	
IP	
[50.87.148.157]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01047-01/	
https://www.csirt.gob.cl/media/2022/01/8FFR22-01047-01.pdf	

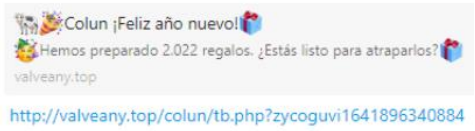
https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Phishing

CSIRT advierte phishing que proviene supuestamente de Zimbra	
Alerta de seguridad cibernética	8FPH21-00460-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2022
Última revisión	11 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
http://digitalinfluencerelite[.]com/wp-content/plugins/verify.php	
IP	
[187.32.63.166]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00460/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00460-01.pdf	

CSIRT informa phishing para canjear puntos supuestamente del Banco Itaú	
Alerta de seguridad cibernética	8FPH21-00461-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de enero de 2022
Última revisión	11 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://itaupersonayempresacl[.]iupp.info/726a292db52f7f5/html/index.php	
IP	
[3.82.199.252]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00461-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00461-01.pdf	

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Imagen del mensaje

http://valveany.top/colun/tb.php?zycoguvi1641896340884

CSIRT advierte phishing con falso concurso que suplanta a Colun	
Alerta de seguridad cibernética	8FPH21-00462-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de enero de 2022
Última revisión	12 de enero de 2022
Indicadores de compromiso	
URL sitio falso	
https://efficientonly[.]top/FqUoFeLq/colun/?_t=1641906819696#1641906825776	
IP	
[104.21.39.91]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00462-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00462-01.pdf	

Imagen del mensaje


CSIRT informa smishing con supuesta ingreso a canal digital del Banco de Chile	
Alerta de seguridad cibernética	8FPH21-00463-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2022
Última revisión	13 de enero de 2022
Indicadores de compromiso	
URL redirección	
https://bitly/SEGURIDAD-BDCH	
URL sitio falso	
https://soporte-cliente.cl.adaisoluciones[.]com/1642016263/bcochile-web/persona/login/index.html/login	
IP	
[70.32.23.57]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00463-01/	
https://www.csirt.gob.cl/media/2022/01/8FPH22-00463-01.pdf	

Vulnerabilidades

CSIRT alerta de vulnerabilidades en Google Android		
Alerta de seguridad cibernética	9VSA21-00544-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	10 de enero de 2022	
Última revisión	10 de enero de 2022	
CVE		
CVE-2021-30319	CVE-2021-30285	CVE-2021-31890
CVE-2021-30311	CVE-2021-30353	CVE-2021-31346
CVE-2021-30308	CVE-2021-1049	CVE-2021-31345
CVE-2021-30307	CVE-2021-0959	CVE-2021-39633
CVE-2021-30301	CVE-2021-31889	CVE-2021-39634
CVE-2021-30300	CVE-2021-40148	CVE-2020-29368
CVE-2021-30287		
Fabricante		
Google		
Productos afectados		
Google Android 9 2021-09-01 a 12 2022-01-01		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00544-01/		
https://www.csirt.gob.cl/media/2022/01/9VSA22-00544-01.pdf		

CSIRT comparte vulnerabilidades Microsoft Update Tuesday Enero 2022		
Alerta de seguridad cibernética	9VSA21-00545-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	12 de enero de 2022	
Última revisión	12 de enero de 2022	
CVE		
CVE-2021-22947	CVE-2022-21869	CVE-2022-21902
CVE-2021-36976	CVE-2022-21870	CVE-2022-21903
CVE-2022-21833	CVE-2022-21871	CVE-2022-21904
CVE-2022-21834	CVE-2022-21872	CVE-2022-21905
CVE-2022-21835	CVE-2022-21873	CVE-2022-21906
CVE-2022-21836	CVE-2022-21874	CVE-2022-21907
CVE-2022-21837	CVE-2022-21875	CVE-2022-21908
CVE-2022-21838	CVE-2022-21876	CVE-2022-21910
CVE-2022-21839	CVE-2022-21877	CVE-2022-21911
CVE-2022-21840	CVE-2022-21878	CVE-2022-21912

CVE-2022-21841	CVE-2022-21879	CVE-2022-21913
CVE-2022-21842	CVE-2022-21880	CVE-2022-21914
CVE-2022-21843	CVE-2022-21881	CVE-2022-21915
CVE-2022-21846	CVE-2022-21882	CVE-2022-21916
CVE-2022-21847	CVE-2022-21883	CVE-2022-21917
CVE-2022-21848	CVE-2022-21884	CVE-2022-21918
CVE-2022-21849	CVE-2022-21885	CVE-2022-21919
CVE-2022-21850	CVE-2022-21887	CVE-2022-21920
CVE-2022-21851	CVE-2022-21888	CVE-2022-21921
CVE-2022-21852	CVE-2022-21889	CVE-2022-21922
CVE-2022-21855	CVE-2022-21890	CVE-2022-21924
CVE-2022-21857	CVE-2022-21891	CVE-2022-21925
CVE-2022-21858	CVE-2022-21892	CVE-2022-21928
CVE-2022-21859	CVE-2022-21893	CVE-2022-21932
CVE-2022-21860	CVE-2022-21894	CVE-2022-21958
CVE-2022-21861	CVE-2022-21895	CVE-2022-21959
CVE-2022-21862	CVE-2022-21896	CVE-2022-21960
CVE-2022-21863	CVE-2022-21897	CVE-2022-21961
CVE-2022-21864	CVE-2022-21898	CVE-2022-21962
CVE-2022-21865	CVE-2022-21899	CVE-2022-21963
CVE-2022-21866	CVE-2022-21900	CVE-2022-21964
CVE-2022-21867	CVE-2022-21901	CVE-2022-21969
CVE-2022-21868		

Fabricante

Microsoft

Productos afectados

Dynamics 365 Sales
HEVC Video Extensions
Microsoft .NET Framework 2.0 Service Pack 2
Microsoft .NET Framework 3.5
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 3.5 AND 4.7.2
Microsoft .NET Framework 3.5 AND 4.8
Microsoft .NET Framework 3.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2
Microsoft .NET Framework 4.8
Microsoft 365 Apps for Enterprise for 32-bit, 64-bit Systems
Microsoft Dynamics 365 Customer Engagement V9.0, V9.1
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2013 Service Pack 1 (32-bit editions), (64-bit editions)
Microsoft Excel 2016 (32-bit edition), (64-bit edition)
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Exchange Server 2016 Cumulative Update 21, 22
Microsoft Exchange Server 2019 Cumulative Update 10, 11
Microsoft Office 2013 RT Service Pack 1

Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft Office 2019 for 32-bit editions
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for Mac
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft Office LTSC for Mac 2021
Microsoft Office Online Server
Microsoft Office Web Apps Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Microsoft SharePoint Enterprise Server 2016
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2019
Microsoft SharePoint Server Subscription Edition
Microsoft Word 2016 (32-bit edition)
Microsoft Word 2016 (64-bit edition)
Remote Desktop client for Windows Desktop
SharePoint Server Subscription Edition Language Pack
Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit, x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for ARM64-based Systems
Windows 11 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server

Core installation) Windows Server 2008 for x64-based Systems Service Pack 2 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2012 R2 (Server Core installation) Windows Server 2016 Windows Server 2016 (Server Core installation) Windows Server 2019 Windows Server 2019 (Server Core installation) Windows Server 2022 Windows Server 2022 (Server Core installation) Windows Server, version 20H2 (Server Core Installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00545-01/
https://www.csirt.gob.cl/media/2022/01/9VSA22-00545-01.pdf

CSIRT alerta de vulnerabilidades en Mozilla Firefox		
Alerta de seguridad cibernética	9VSA21-00546-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	13 de enero de 2022	
Última revisión	13 de enero de 2022	
CVE		
CVE-2022-22746	CVE-2022-22737	CVE-2022-22744
CVE-2022-22743	CVE-2021-4140	CVE-2022-22747
CVE-2022-22742	CVE-2022-22749	CVE-2022-22736
CVE-2022-22744	CVE-2022-22750	CVE-2022-22739
CVE-2022-22741	CVE-2022-22748	CVE-2022-22751
CVE-2022-22740	CVE-2022-22745	CVE-2022-22752
CVE-2022-22738		
Fabricante		
Mozilla		
Productos afectados		
Mozilla Firefox, versiones anteriores a Firefox 96		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00546-01/		
https://www.csirt.gob.cl/media/2022/01/9VSA22-00546-01.pdf		

CSIRT alerta de vulnerabilidades en productos SAP		
Alerta de seguridad cibernética	9VSA21-00547-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	13 de enero de 2022	
Última revisión	13 de enero de 2022	
CVE		
CVE-2021-44228	CVE-2021-44234	CVE-2021-42070
CVE-2022-22531	CVE-2022-22529	CVE-2021-42069
CVE-2021-44235	CVE-2022-42067	CVE-2021-44233
CVE-2021-42066	CVE-2021-42068	
Fabricante		
SAP		
Productos afectados		
SAP Customer Checkout. SAP BTP Cloud Foundry SAP Landscape Management. SAP Connected Health Platform 2.0 – Fhirserver. SAP HANA XS Advanced Cockpit. SAP NetWeaver Process Integration (Java Web Service Adapter). SAP HANA XS Advanced. Internet of Things Edge Platform. SAP BTP Kyma. SAP Enable Now Manager. SAP Cloud for Customer (add-in for Lotus notes client). SAP Localization Hub, digital compliance service for India. SAP Edge Services On Premise Edition. SAP Edge Services Cloud Edition. SAP BTP API Management (Tenant Cloning Tool). SAP NetWeaver ABAP Server and ABAP Platform (Adobe LiveCycle Designer 11.0). SAP Digital Manufacturing Cloud for Edge Computing. SAP Enterprise Continuous Testing by Tricentis. SAP Cloud-to-Cloud Interoperability. Reference Template for enabling ingestion and persistence of time series data in Azure. SAP Business One.		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00547-01/		
https://www.csirt.gob.cl/media/2022/01/9VSA22-00547-01.pdf		

CSIRT alerta de nuevas vulnerabilidades en productos de Adobe		
Alerta de seguridad cibernética	9VSA21-00548-01	
Clase de alerta	Vulnerabilidad	
Tipo de incidente	Sistema y/o Software Abierto	
Nivel de riesgo	Alto	
TLP	Blanco	
Fecha de lanzamiento original	13 de enero de 2022	
Última revisión	13 de enero de 2022	
CVE		
CVE-2021-44715	CVE-2021-44701	CVE-2021-44187
CVE-2021-45068	CVE-2021-44713	CVE-2021-44186
CVE-2021-45067	CVE-2021-44712	CVE-2021-44185
CVE-2021-45064	CVE-2021-44711	CVE-2021-44743
CVE-2021-45063	CVE-2021-44710	CVE-2021-45051
CVE-2021-45062	CVE-2021-44709	CVE-2021-45052
CVE-2021-45061	CVE-2021-44708	CVE-2021-43752
CVE-2021-45060	CVE-2021-44707	CVE-2021-44700
CVE-2021-44742	CVE-2021-44706	CVE-2021-45053
CVE-2021-44741	CVE-2021-44705	CVE-2021-45056
CVE-2021-44740	CVE-2021-44704	CVE-2021-45054
CVE-2021-44739	CVE-2021-44703	CVE-2021-45055
CVE-2021-44714	CVE-2021-44702	
Fabricante		
Adobe		
Productos afectados		
Adobe Acrobat: 2015.006.30503 a 2017.011.30204 Adobe Acrobat Reader: 2015.006.30508 a 2017.011.30204 Adobe Acrobat DC: 2020.001.30020 a 2021.007.20099 Adobe Acrobat Reader DC: 2020.001.30020 a 2021.007.20099 Adobe Bridge CC 11.0.0 a 12.0. Adobe Illustrator CC 25.0.1 a 26.0.1. Adobe InCopy 16.0.0 a 16.4		
Enlaces para revisar el informe:		
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00548-01/		
https://www.csirt.gob.cl/media/2022/01/9VSA22-00548-01.pdf		

CSIRT alerta de nuevas vulnerabilidades en productos de Cisco	
Alerta de seguridad cibernética	9VSA21-00549-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de enero de 2022
Última revisión	13 de enero de 2022

CVE

CVE-2022-20658	CVE-2022-20633	CVE-2022-20641
CVE-2022-20652	CVE-2022-20634	CVE-2022-20642
CVE-2022-20663	CVE-2022-20635	CVE-2022-20643
CVE-2022-20626	CVE-2022-20636	CVE-2022-20644
CVE-2022-20656	CVE-2022-20637	CVE-2022-20645
CVE-2022-20657	CVE-2022-20638	CVE-2022-20646
CVE-2022-20660	CVE-2022-20639	CVE-2022-20647
CVE-2022-20631	CVE-2022-20640	CVE-2022-20651
CVE-2022-20632		

Fabricante

Cisco

Productos afectados

Cisco Unified CCMP y Cisco Unified CCDM
Cisco Tetration
Cisco Secure Network Analytics
Cisco Prime Access Registrar Appliance
Cisco Prime Infrastructure and Evolved Programmable Network Manager
Cisco IP Phones
Cisco Enterprise Chat and Email
Cisco Adaptive Security Device Manager

Enlaces para revisar el informe:

https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00549-01/
https://www.csirt.gob.cl/media/2022/01/9VSA22-00549-01.pdf

Actualidad

Ciberconsejos para un verano más seguro

Aunque estés de vacaciones, nunca debes relajar tu ciberseguridad. Por eso, sigue estos consejos y no pases malos ratos que interrumpan tu descanso veraniego, sea que salgas de tu casa o no. También los puedes encontrar aquí: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-verano2022/.

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.

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob

Muro de la Fama

El siguiente es el listado de personas y organizaciones que han colaborado explícitamente con el CSIRT de Gobierno para mejorar la seguridad informática en instituciones y organismos del Estado, al informar problemas de seguridad y vulnerabilidades descubiertas.

El CSIRT de Gobierno destaca en este segmento a quienes reportaron incidentes utilizando canales formales (https://www.csirt.gob.cl o al teléfono +(562) 2486 3850) siempre que hayan aportado información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución de este.

- José Ignacio Parra
- Bendercito

https://www.csirt.gob.cl + (562) 2486 3850 @csirtgob @CSIRTConciencia https://www.linkedin.com/company/csirt-gob