Ministerio del Interior y Seguridad Pública

12-07-2022 | Año 4 | N°162

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Boletín de Seguridad Cibernética

Semana del 5 al 11 de agosto de 2022

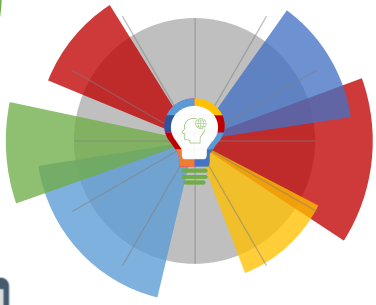
La semana en cifras

Parches

152

para vulnerabilidades

Sus mitigaciones son útiles en productos de Bosch, Cisco, Microsoft, Apache y VMware,



Hash

23

SHA

Asociadas a múltiples campañas de phishing con archivos que contienen malware

Se advirtieron

15

URL

Asociadas a sitios fraudulentos y campañas de phishing y malware.

IP

12

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

Sitios fraudulentos

Imagen del sitio

CSIRT advierte sitio falso que suplanta al Banco Santander	
Alerta de seguridad cibernética	8FFR22-01094-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de agosto de 2022
Última revisión	8 de agosto de 2022
Indicadores de compromiso	
URL sitio falso	
hxxps://santandermovil.maderacco.com.br/1659965294/portada/personas/home.asp	
IP	
[109.106.251.203]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr22-01094-01/	
https://www.csirt.gob.cl/media/2022/08/8FFR22-01094-01.pdf	

Phishing

Imagen del mensaje

CSIRT advierte phishing que suplanta al Banco Ripley	
Alerta de seguridad cibernética	8FPH22-00569-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de agosto de 2022
Última revisión	5 de agosto de 2022
Indicadores de compromiso	
URL Redirección	
https://bit[.]ly/3JmnxGR	
hXXp://68.183.93.132/4cd75b3c153e177dee34be6e404661a4/18c98448d847f76216f245e5980b7d02/8dad4LIYCL/	
URL sitio falso	
https://autoatencion-banco-estado[.]cf/personales?253c52d5md16p2gjekglb1	
IP	
[103.41.204.175]	
[204.11.58.233]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00569-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00569-01.pdf	

Imagen del mensaje

CSIRT advierte phishing que suplanta al correo Zimbra	
Alerta de seguridad cibernética	8FPH22-00570-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
Indicadores de compromiso	
URL Redirección	
Evos[.]imgix.net	
URL sitio falso	
https://karen-carter.kizen.com/form/5S2mma7K	
IP	
[192.168.0.24]	
[109.106.251.203]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00570-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00570-01.pdf	

Imagen del mensaje

CSIRT advierte phishing con falsa actualización de datos de correo	
Alerta de seguridad cibernética	8FPH22-00571-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
Indicadores de compromiso	
URL Redirección	
evos.imgix.net	
URL sitio falso	
https://cimensavenimweb.wapka.co/	
IP	
[190.52.187.217]	
[109.106.251.203]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00571-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00571-01.pdf	

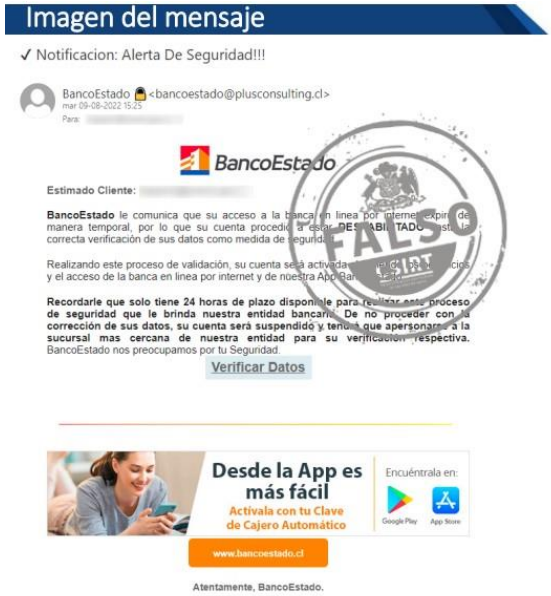
Imagen del mensaje

CSIRT informa phishing que suplanta a un Departamento de Recursos Humanos	
Alerta de seguridad cibernética	8FPH22-00572-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
Indicadores de compromiso	
URL Redirección	
https://confident-raman.163-123-143-94.plesk.page/aVSaSKXkEZZtHhGD8N79MBVSNyMxy9rAfixedibmxdmFjLXBhZ2V4LWxkbHFnZm9wemtva3dsYW5kcWN2d3pnZ3FpZmV0Y2h4c29jaXNlY3VyZWR4aW50ZXJpb3IuZ29iLmNs	
URL sitio falso	
https://heuristic-bardeen.163-123-143-94.plesk.page/fJquD5KD3XG5FBv3zsL7CteiOSwNypQcibmxdmFjLXBhZ2V4LXBvdG9hZWxwb3RvYWVscG90b2FlbHBvdG9hZWxwb3RvYWVsLWRvYy1zb2MtcmV4LWludGVyaW9yLmdvYi5jbA==	
IP	
[143.110.226.244]	
[163.123.143.94]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00572-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00572-01.pdf	

Imagen del mensaje

CSIRT alerta phishing que suplanta al Banco de Chile	
Alerta de seguridad cibernética	8FPH22-00573-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
Indicadores de compromiso	
URL Redirección	
https://tinyurl.com/yv7cu79f	
https://qiotic.com/rrcl/?32	
URL sitio falso	
https://portalacceso.bancochlle.cl.codeticsa.com/	
IP	
[18.157.163.194]	
[67.23.226.158]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00573-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00573-01.pdf	

Imagen del mensaje



CSIRT alerta de campaña de phishing que suplanta al BancoEstado	
Alerta de seguridad cibernética	8FPH22-00574-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
Indicadores de compromiso	
URL Redirección	
https://s3rvicu4ck.com/activacion/cuenta-lwnr/	
URL sitio falso	
http://simpeg.unhi.ac.id/1660079023/Login	
IP	
[172.104.45.98]	
[45.7.231.99]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph22-00574-01/	
https://www.csirt.gob.cl/media/2022/08/8FPH22-00575-01-1.pdf	

Malware

CSIRT advierte phishing con malware con falsos informes	
Alerta de seguridad cibernética	2CMV22-00308-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de agosto de 2022
Última revisión	5 de agosto de 2022
Indicadores de compromiso	
Hash	
ba7d5d9d39a8b0518c4c7fc9f57ce1152ccfaf3351b04396206a6a04f91a29c9	
351fbe08be27e287be997f6864fd4d37d7ceffd5d44b9ad3b19b3ad7745cdd0a	
aa4ceb691665ca0a488de61e9fc863b994c28d8ed9beca5891eeb3dd9a42bd9c	
eb858be4fa2d838a05a9f72a82bcf712dd6038e2fe3e502d2a4497a879bbc544	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00308-01/	
https://www.csirt.gob.cl/media/2022/08/2CMV22-00308-01.pdf	

CSIRT advierte phishing con malware que suplanta a Heinz Glas	
Alerta de seguridad cibernética	2CMV22-00309-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
Indicadores de compromiso	
Hash	
1eb8d76fd884aa3574449f0e7f3d7551e670f0f181252d669b717e29c35db3c5	
a5587070de0961536ff5d59569a7733fd58f74953a69bfd46e3c38cabb95d378	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/2cmv22-00309-01/	
https://www.csirt.gob.cl/media/2022/08/2CMV22-00309-01.pdf	

Imagen del mensaje	CSIRT informa phishing con malware suplantando a Solutionmarkers	
	Alerta de seguridad cibernética	2CMV22-00310-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	9 de agosto de 2022
	Última revisión	9 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	20044bc3515379b70e4d42b57ff3ac32d5b590a0d185c8b5da2cea830f3368ed	
	2e72514a05ff383452a3dc1f1a8be040c3a1ebc23a224dc480064322efb85eb7	
	401eb0cdb84e642291539b684b9da7128c07ec540649753a7ae4e72b8f1910b3	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv2-00310-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00310-01.pdf	

Imagen del mensaje	CSIRT informa campaña de phishing con malware con falsa orden de compra	
	Alerta de seguridad cibernética	2CMV22-00311-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de agosto de 2022
	Última revisión	10 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	1f68c494a47fe68c7346e5a67e53c3fd7eaae9030ad281188938f2d6e40013d6	
	6b8b620534b94530ba467af917e0365640b83b1edd8a39eaa00ebf441e2e34c0	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00310-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00311-01.pdf	

Imagen del mensaje	CSIRT informa phishing con malware con falso documento de pago	
	Alerta de seguridad cibernética	2CMV22-00312-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de agosto de 2022
	Última revisión	10 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	3b8eee0670ee9f2f320c448b9222122fa97ba784b63ff156d035a622bf97c9aa	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00312-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00312-01.pdf	

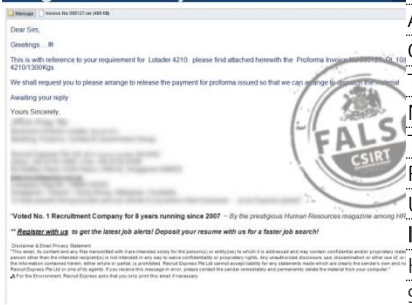
Imagen del mensaje	CSIRT advierte phishing con malware con falsa factura	
	Alerta de seguridad cibernética	2CMV22-00313-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de agosto de 2022
	Última revisión	10 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	92e9972dd21c2eaf4412353e49f151b45293b8c153589e77bdb4006ac5ce9af0	
	b8b0c0f52da53d3269ee344c46166f7d5daeaf6887ba0f98545f45aa1eb1ba21	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00313-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00313-01.pdf	

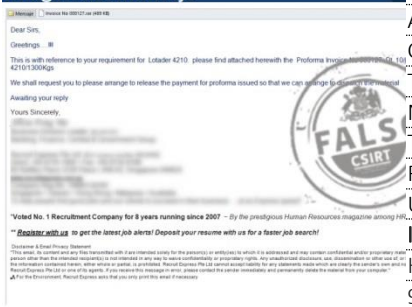
Imagen del mensaje	CSIRT advierte phishing con malware con falsa factura	
	Alerta de seguridad cibernética	2CMV22-00313-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de agosto de 2022
	Última revisión	10 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	92e9972dd21c2eaf4412353e49f151b45293b8c153589e77bdb4006ac5ce9af0	
	b8b0c0f52da53d3269ee344c46166f7d5daeaf6887ba0f98545f45aa1eb1ba21	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00313-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00313-01.pdf	

Imagen del mensaje	CSIRT alerta campaña de phishing con malware en falso documento de pago	
	Alerta de seguridad cibernética	2CMV22-00314-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de agosto de 2022
	Última revisión	10 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	97961c60aad3ead4d3d5ea0de55fd5778a577663cb60879dabf8a90d60ca91af	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00314-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00314-PH-01.pdf	

Imagen del Mensaje	CSIRT alerta de campañas de phishing con malware en falso documento de pago	
	Alerta de seguridad cibernética	2CMV22-00315-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	10 de agosto de 2022
	Última revisión	10 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	1f7aad9b4c0fe5920c99c3dd8671f8c5bf2fb64dab045f765eac602148788 61c	
	03b4f9aa816b75952a1dc1634d6c4248a6ab92990b8e4d70efecef1c05c3674 2	
	61258f0cfb236b3b532380b64c8aa2c9ab02c8b5022df8beca51d1d6a493b57 e	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00315-01/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00315-PH-01.pdf	

Imagen del Mensaje	CSIRT advierte phishing con malware con falsa factura	
	Alerta de seguridad cibernética	2CMV22-00316-01
	Clase de alerta	Fraude
	Tipo de incidente	Malware
	Nivel de riesgo	Alto
	TLP	Blanco
	Fecha de lanzamiento original	11 de agosto de 2022
	Última revisión	11 de agosto de 2022
	Indicadores de compromiso	
	Hash	
	940e765d2f5f96c90f0ac044eef945b13d0f7093448fcd9e1669054c544414b0	
	702a898f99fdcf56d29f5a9d4c54794c09880f7b000488a1f9f4c2259e520bee	
	a4944f1c7e67aa8cf68ecdeb2c74e3c60537b6ca3c5d57b6958d6dab791fffc6	
	Enlaces para revisar el informe:	
	https://www.csirt.gob.cl/alertas/2cmv22-00316-ph/	
	https://www.csirt.gob.cl/media/2022/08/2CMV22-00316-PH-01.pdf	

Vulnerabilidades

CSIRT comparte vulnerabilidades en productos de Bosch	
Alerta de seguridad cibernética	9VSA22-00685-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	8 de agosto de 2022
Última revisión	8 de agosto de 2022
CVE	
CVE-2022-36301 CVE-2022-36302	
Fabricantes	
Bosch	
Productos afectados	
Bosch BF-OS 3.x La vulnerabilidad es eliminada en BF-OS versión 3.84.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00685-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00685-01.pdf	

CSIRT comparte vulnerabilidades del Update Tuesday de Microsoft para agosto 2022	
Alerta de seguridad cibernética	9VSA22-00686-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	9 de agosto de 2022
Última revisión	9 de agosto de 2022
CVE	
CVE-2022-35794 - CVE-2022-35766 - CVE-2022-35804 CVE-2022-35767 - CVE-2022-35753 - CVE-2022-35752 CVE-2022-35745 - CVE-2022-35744 - CVE-2022-34714 CVE-2022-34702 - CVE-2022-34696 - CVE-2022-34691 CVE-2022-33646 - CVE-2022-30133 - CVE-2022-24477 CVE-2022-24516 - CVE-2022-21980 - CVE-2022-35771 CVE-2022-34717 - CVE-2022-35768 - CVE-2022-35792 CVE-2022-35765 - CVE-2022-35764 - CVE-2022-35760 CVE-2022-35754 - CVE-2022-35795 - CVE-2022-35772 CVE-2022-35797 - CVE-2022-35763 - CVE-2022-35820 CVE-2022-35779 - CVE-2022-35806 - CVE-2022-35819	

CVE-2022-35818 - CVE-2022-35791 - CVE-2022-35817 CVE-2022-35816 - CVE-2022-35790 - CVE-2022-35815 CVE-2022-35789 - CVE-2022-35814 - CVE-2022-35784 CVE-2022-35783 - CVE-2022-35809 - CVE-2022-35782 CVE-2022-35808 - CVE-2022-35807 - CVE-2022-35781 CVE-2022-35780 - CVE-2022-35777 - CVE-2022-34703 CVE-2022-33670 - CVE-2022-35793 - CVE-2022-35802 CVE-2022-35776 - CVE-2022-35801 - CVE-2022-35775 CVE-2022-35800 - CVE-2022-35774 - CVE-2022-35799 CVE-2022-35769 - CVE-2022-35826 - CVE-2022-35825 CVE-2022-35824 - CVE-2022-35757 - CVE-2022-35827 CVE-2022-34303 - CVE-2022-34692 - CVE-2022-35762 CVE-2022-35821 - CVE-2022-35788 - CVE-2022-35813 CVE-2022-35787 - CVE-2022-35786 - CVE-2022-35812 CVE-2022-35785 - CVE-2022-35811 - CVE-2022-35810 CVE-2022-35773 - CVE-2022-34686 - CVE-2022-30176 CVE-2022-30175 - CVE-2022-34685 - CVE-2022-35761 CVE-2022-35759 - CVE-2022-35758 - CVE-2022-35756 CVE-2022-35755 - CVE-2022-35751 - CVE-2022-35750 CVE-2022-35749 - CVE-2022-35748 - CVE-2022-35747 CVE-2022-35746 - CVE-2022-35743 - CVE-2022-35742 CVE-2022-34716 - CVE-2022-34715 - CVE-2022-34713 CVE-2022-34712 - CVE-2022-34710 - CVE-2022-34709 CVE-2022-34708 - CVE-2022-34707 - CVE-2022-34706 CVE-2022-34705 - CVE-2022-34704 - CVE-2022-34701 CVE-2022-33640 - CVE-2022-34699 - CVE-2022-34690 CVE-2022-34687 - CVE-2022-33648 - CVE-2022-33631 CVE-2022-34302 - CVE-2022-30194 - CVE-2022-30144 CVE-2022-30134 - CVE-2022-21979 - CVE-2022-30197 CVE-2022-34301
Fabricante
Microsoft
Productos afectados
Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 21H2 for ARM64-based Systems Windows 10 Version 21H2 for 32-bit Systems Windows 11 for ARM64-based Systems Windows 11 for x64-based Systems Windows Server, version 20H2 (Server Core Installation) Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for x64-based Systems Windows Server 2022 (Server Core installation) Windows Server 2022 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 Server 2019 (Server Core installation) Windows Server 2019 Windows 10 Version 1809 for ARM64-based Systems

Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2016 (Server Core installation)
Windows Server 2016
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Azure Batch
Microsoft Exchange Server 2016 Cumulative Update 23
Microsoft Exchange Server 2019 Cumulative Update 12
Microsoft Exchange Server 2019 Cumulative Update 11
Microsoft Exchange Server 2016 Cumulative Update 22
Microsoft Exchange Server 2013 Cumulative Update 23
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Microsoft Office 2013 RT Service Pack 1
Microsoft Office 2016 (32-bit edition)
Microsoft Office 2016 (64-bit edition)
Microsoft 365 Apps for Enterprise for 32-bit Systems
Microsoft Office LTSC 2021 for 32-bit editions
Microsoft Office LTSC 2021 for 64-bit editions
Microsoft 365 Apps for Enterprise for 64-bit Systems
Microsoft Office 2019 for 64-bit editions
Microsoft Office 2019 for 32-bit editions
Azure Site Recovery VMWare to Azure
Azure Real Time Operating System GUIX Studio
Microsoft Visual Studio 2015 Update 3
Microsoft Visual Studio 2013 Update 5
Microsoft Visual Studio 2012 Update 5
Microsoft Visual Studio 2022 version 17.0
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 – 16.10)

Microsoft Visual Studio 2019 version 16.9 (includes 16.0 – 16.8)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 – 15.8)
Microsoft Visual Studio 2022 version 17.2
Azure Sphere
Microsoft Outlook 2013 RT Service Pack 1
Microsoft Outlook 2013 Service Pack 1 (64-bit editions)
Microsoft Outlook 2013 Service Pack 1 (32-bit editions)
Microsoft Outlook 2016 (64-bit edition)
Microsoft Outlook 2016 (32-bit edition)
.NET Core 3.1
.NET 6.0
System Center Operations Manager (SCOM) 2022
System Center Operations Manager (SCOM) 2016
System Center Operations Manager (SCOM) 2019
Microsoft Office Online Server
Open Management Infrastructure
Microsoft Excel 2013 Service Pack 1 (64-bit editions)
Microsoft Excel 2013 Service Pack 1 (32-bit editions)
Microsoft Excel 2013 RT Service Pack 1
Microsoft Excel 2016 (64-bit edition)
Microsoft Excel 2016 (32-bit edition)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00686-01/
https://www.csirt.gob.cl/media/2022/08/9VSA22-00686-01.pdf

CSIRT comparte nuevas vulnerabilidades de Cisco	
Alerta de seguridad cibernética	9VSA22-00687-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2022
Última revisión	10 de agosto de 2022

CVE

CVE-2022-20798
CVE-2022-20869
CVE-2022-20816
CVE-2022-20914
CVE-2022-20820
CVE-2022-20852
CVE-2022-20827
CVE-2022-20841
CVE-2022-20842
CVE-2021-1585
CVE-2022-20713
CVE-2022-20829
CVE-2022-20866
CVE-2022-20715

Fabricante

Cisco

Productos afectados

RV160 VPN Routers
RV160W Wireless-AC VPN Routers
RV260 VPN Routers
RV260P VPN Routers with PoE
RV260W Wireless-AC VPN Routers
RV340 Dual WAN Gigabit VPN Routers
RV340W Dual WAN Gigabit Wireless-AC VPN Routers
RV345 Dual WAN Gigabit VPN Routers
RV345P Dual WAN Gigabit POE VPN Routers
Cisco Secure Email and Web Manager
Cisco ASA Software Release
Cisco FTD Software Release
ASA 5506-X with FirePOWER Services
ASA 5506H-X with FirePOWER Services
ASA 5506W-X with FirePOWER Services
ASA 5508-X with FirePOWER Services
ASA 5516-X with FirePOWER Services
Firepower 1000 Series Next-Generation Firewall
Firepower 2100 Series Security Appliances
Firepower 4100 Series Security Appliances
Firepower 9300 Series Security Appliances
Secure Firewall 3100

Aparatos Cisco si corren una edición del Cisco ASA Software anterior a la 9.17(1) y tienen activado Clientless SSL VPN Aparatos Cisco si corren una edición del Cisco ASA Software anterior a 9.16.3.19, 9.17.1.13, o 9.18.2., el aparato está configurado con una versión Cisco ASDM anterior a la 7.18.1.152., la imagen Cisco ASDM usa un lCisco ASDM-IDM Launcher anterior a la versión 1.9(5) y el aparato está configurado para acceso de administración HTTPS Cisco ASDM, ediciones anteriores a 7.18.1.152 Cisco Webex Meetings Cisco Identity Service Engine (ISE) Software Cisco Unified CM y Cisco Unified CM SME Cisco BroadWorks Application Delivery Platform Software
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00687-01/
https://www.csirt.gob.cl/media/2022/08/9VSA22-00687-01.pdf

CSIRT comparte vulnerabilidades en Apache Traffic Server	
Alerta de seguridad cibernética	9VSA22-00688-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	10 de agosto de 2022
Última revisión	10 de agosto de 2022
CVE	
CVE-2021-37150 CVE-2022-25763 CVE-2022-28129 CVE-2022-31780 CVE-2022-31778	
Fabricante	
Apache	
Productos afectados	
Apache Traffic Server 8.0.0 a 9.1.2	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00688-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00688-01.pdf	

CSIRT alerta de vulnerabilidades en productos VMware	
Alerta de seguridad cibernética	9VSA22-00689-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de agosto de 2022
Última revisión	11 de agosto de 2022
CVE	
CVE-2022-31656 CVE-2022-31657 CVE-2022-31658 CVE-2022-31659 CVE-2022-31660 CVE-2022-31661 CVE-2022-31662 CVE-2022-31663 CVE-2022-31664 CVE-2022-31665	
Fabricante	
VNware	
Productos afectados	
VMware Workspace ONE Access VMware Workspace ONE Access Connector VMware Identity Manager VMware Identity Manager Connector VMware vRealize Automation VMware Cloud Foundation VMware vRealize Suite Lifecycle Manager	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa22-00689-01/	
https://www.csirt.gob.cl/media/2022/08/9VSA22-00689-01.pdf	

Actualidad

Ciberdiccionario Volumen 13

En el marco de la celebración del Mes del Niño y de la Niña, preparamos una nueva versión del ciberdiccionario con algunos términos que se utilizan en las redes sociales como hater, hashtag, influencer y trolear.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberdiccionario-volumen-13/

Ciberconsejos | Juegos conectados: ¿Qué son y cómo jugar seguros?

Los juguetes conectados a internet o que interactúan con otros dispositivos pueden buscar información en línea de manera inmediata, intercambiar datos e interactuar con otros dispositivos, como smartphones o tablets. Entre sus principales funcionalidades están:

- Navegar o comunicarse a través de Internet.
- Transmitir o grabar vídeos en tiempo real.
- Grabar, reproducir o reconocer la voz.
- Interactuar con una aplicación en un smartphone o tablet.

Lo anterior hacer que este tipo de juguetes presentes riesgos, como entregar datos personales del niño o de su familia disponible en el juguete, en la aplicación vinculada al juguete o al juego online al que está conectado el juguete. Además de existir la posibilidad de dar acceso no controlado al juguete a desconocidos o incluso el riesgo también de grabaciones de vídeos o audios de otras personas sin autorización.

¿Cómo mantener seguro a tu hijo si ya tiene este tipo de juegos? Te contamos en el video disponible en el siguiente enlace: https://www.csirt.gob.cl/recomendaciones/juegos-conectados-que-son-y-como-jugar-seguros/

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.

- Montserrat Badal
- Jhony Gómez
- Camila Saa
- Gaspar Salvatierra
- Juan Pablo Berríos
- Cristián Medina
- Janito Muñoz
- Jacqueline Sánchez
- Felipe Montenegro
- Gonzalo Jerez
- Miguel Valenzuela
- Fernanda Ascencio
- Bernardo Martínez
- Ferenc Riquelme
- Rodrigo Silva