CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

14-01-2021 | Año 3 | N°80

Boletín de Seguridad Cibernética

Semana del 07 al 13 de Enero de 2021

División de Redes y Seguridad Informática. Gobierno de Chile

Ministerio del Interior y Seguridad Pública Gobierno de Chile

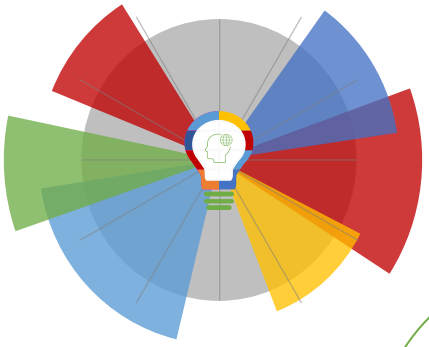
Resumen de la semana en cifras

Hash

5

Sha 256

Asociadas a múltiples campañas de phishing con archivos que contienen malware



Se advirtieron

7

URLs

Asociadas a sitios fraudulentos y campañas de phishing

Parches

223

para vulnerabilidades

Las mitigaciones son útiles para productos Nvidia, Mozilla, Google, Fortinet, Tensor Flow, PHP, GitLab, Opera mini, Microsoft, Joomla y Red Hat.

IPs

14

Informadas

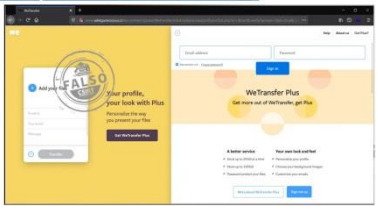
Listado de IPs advertidas en múltiples campañas de phishing y de malware.

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

Contenido

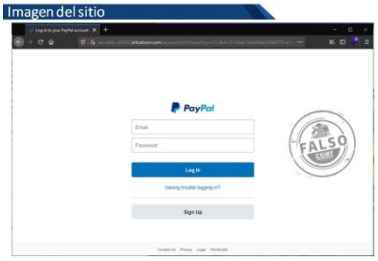
Sitios fraudulentos

Imagen del sitio



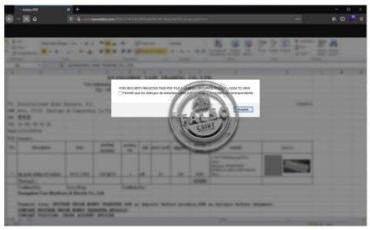
CSIRT advierte sitio fraudulento de transferencia de archivos	
Alerta de seguridad cibernética	8FFR21-00870-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2021
Última revisión	08 de Enero de 2021
Indicadores de compromiso	
URL	
http://www.adelgacecorpus.cl/wp-content/global/Wetransfer	
IP	
200[.]73.113.171	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00870-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00870-01.pdf	

Imagen del sitio



CSIRT advierte suplantación de sitio de sistema de pagos en línea	
Alerta de seguridad cibernética	8FFR21-00871-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Enero de 2021
Última revisión	11 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//acc-eslin-40365.bitballoon[.]com/account.html?country.x=CL&id=3193de1b656fde259b4751a3590a835a&cmd=signin	
IP	
104[.]248.63.248	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00871-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00871-01.pdf	

Imagen del sitio



CSIRT informa sitio fraudulento de compañía de software	
Alerta de seguridad cibernética	8FFR21-00872-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Enero de 2021
Última revisión	11 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//www.tawreedss[.]com/PDF/27f410028f3fc4d4fb3f61f6ee2b6791/index.pdf.html	
IP	
192[.]232.249.142	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00872-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00872-01.pdf	

Imagen del sitio

CSIRT advierte página de servicio de correo falsa	
Alerta de seguridad cibernética	8FFR21-00873-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Enero de 2021
Última revisión	13 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//exporteas[.]cl/office/outlookweb/mail.crayon.com/owa/auth/logon74bd.html	
IP	
162[.]241.130.204	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8ffr21-00873-01/	
https://www.csirt.gob.cl/media/2021/01/8FFR21-00873-01.pdf	

Phishing

Imagen del mensaje

CSIRT informa phishing por una supuesta SúperClave inactiva	
Alerta de seguridad cibernética	8FPH21-00350-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2021
Última revisión	07 de Enero de 2021
Indicadores de compromiso	
URL	
https://santander.personascl[.]online/1609946968/index.asp	
IP	
[108.166.219.79]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00350-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00350-01.pdf	

Imagen del mensaje

CSIRT advierte phishing de SúperClave bloqueada	
Alerta de seguridad cibernética	8FPH21-00351-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2021
Última revisión	07 de Enero de 2021
Indicadores de compromiso	
URL	
https[:]//www.saantandercl-personas[.]com/1610028620/index.asp	
IP	
[108.166.219.79]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00351-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00351-01.pdf	

Imagen del mensaje

CSIRT informa phishing con supuesto avance en efectivo aprobado	
Alerta de seguridad cibernética	8FPH21-00352-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de Enero de 2021
Última revisión	13 de Enero de 2021
Indicadores de compromiso	
URL	
http[:]//scotiapersonal-cl.computekstr[.]com/45fdf968ef42f346ebfe7245a3d03372/login/personas	
IP	
[92.223.65.46]	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/alertas/8fph21-00352-01/	
https://www.csirt.gob.cl/media/2021/01/8FPH21-00352-01-1.pdf	

Vulnerabilidades

CSIRT comparte mitigaciones entregadas por Mozilla	
Alerta de seguridad cibernética	9VSA21-00353-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2021
Última revisión	07 de Enero de 2021
CVE	
CVE-2020-16044	
Fabricante	
Mozilla	
Productos afectados	
Firefox, Firefox ESR y Firefox para Android.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00353-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00353-01.pdf	

CSIRT comparte vulnerabilidades obtenidas por Google	
Alerta de seguridad cibernética	9VSA21-00354-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2021
Última revisión	07 de Enero de 2021
CVE	
CVE-2021-21106 - CVE-2021-21107 - CVE-2021-21108 CVE-2021-21109 - CVE-2021-21110 - CVE-2021-21111 CVE-2021-21112 - CVE-2021-21113 - CVE-2020-16043 CVE-2021-21114 - CVE-2020-15995 - CVE-2021-21115 CVE-2021-21116	
Fabricante	
Google	
Productos afectados	
Google Chrome versiones anteriores a la 87.0.4280.141 en Windows, Linux y Mac.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00354-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00354-01.pdf	

CSIRT comparte mitigaciones entregadas por Fortinet	
Alerta de seguridad cibernética	9VSA21-00355-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Enero de 2021
Última revisión	07 de Enero de 2021
CVE	
CVE-2020-29010 - CVE-2020-29016 - CVE-2020-29017 CVE-2020-29018 - CVE-2020-29019	
Fabricante	
Fortinet	
Productos afectados	
FortiGate, versiones 6.0.0 a la 6.4.1. FortiWeb, versiones 6.2.0 a la 6.3.5. FortiDeceptor, versiones 3.0.0, 3.0.1 y 3.1.0. FortiWeb, versiones 6.3.0 a la 6.3.5. FortiWeb, versiones de la 6.2.0 a la 6.3.7	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00355-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00355-01.pdf	

CSIRT informa vulnerabilidades obtenidas de TensorFlow	
Alerta de seguridad cibernética	9VSA21-00356-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2021
Última revisión	08 de Enero de 2021
CVE	
CVE-2020-26266 - CVE-2020-26267 - CVE-2020-26268 CVE-2020-26270 - CVE-2020-26271 - CVE-2020-13790 CVE-2020-15250 - CVE-2019-20838 - CVE-2020-14155	
Fabricante	
Tensor Flow	
Productos afectados	
TensorFlow, versiones 1.0.0 a 2.3.1	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00356-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00356-01.pdf	

CSIRT comparte mitigaciones obtenidas de Nvidia	
Alerta de seguridad cibernética	9VSA21-00357-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	08 de Enero de 2021
Última revisión	08 de Enero de 2021
CVE	
CVE-2021-1051 - CVE-2021-1052 - CVE-2021-1053 CVE-2021-1054 - CVE-2021-1055 - CVE-2021-1056 CVE-2021-1057 - CVE-2021-1058 - CVE-2021-1059 CVE-2021-1060 - CVE-2021-1061 - CVE-2021-1062 CVE-2021-1063 - CVE-2021-1064 - CVE-2021-1065 CVE-2021-1066	
Fabricante	
Tensor Flow	
Productos afectados	
Nvidia GPU Display Driver: GeForce, Nvidia RTX/Quadro, NVS y Tesla, todas las versiones. Para los drivers de Tesla en Linux la actualización será lanzada la semana del 18 de enero, informó Nvidia. Nvidia vGPU: Todas las versiones.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00357-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00357-01.pdf	

CSIRT comparte vulnerabilidades obtenidas de PHP	
Alerta de seguridad cibernética	9VSA21-00358-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de Enero de 2021
Última revisión	09 de Enero de 2021
CVE	
CVE-2020-7071	
Fabricante	
PHP	
Productos afectados	
PHP: Versiones de la 7.3 a la 7.4.13.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00358-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00358-01.pdf	

CSIRT comparte mitigaciones obtenidas de GitLab	
Alerta de seguridad cibernética	9VSA21-00359-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	11 de Enero de 2021
Última revisión	11 de Enero de 2021
CVE	
CVE-2021-22166 - CVE-2020-26414	
Fabricante	
GitLab	
Productos afectados	
GitLab Community Edition: Versiones de la 11.5.0 a la 13.7.1. GitLab Enterprise Edition: Versiones de la 11.5.0. a la 13.7.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00359-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00359-01.pdf	

CSIRT comparte vulnerabilidad de Opera Mini	
Alerta de seguridad cibernética	9VSA21-00360-01
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 2021
Última revisión	12 de Enero de 2021
CVE	
CVE-2021-23253	
Fabricante	
Opera Mini	
Productos afectados	
Opera Mini para Android, versiones anteriores a la 53.1.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00360-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00360-01.pdf	

CSIRT comparte mitigaciones obtenidas de Microsoft	
Alerta de seguridad cibernética	9VSA21-00361-01
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 2021
Última revisión	12 de Enero de 2021

CVE

CVE-2020-26870	CVE-2021-1663	CVE-2021-1707
CVE-2021-1636	CVE-2021-1669	CVE-2021-1708
CVE-2021-1637	CVE-2021-1670	CVE-2021-1711
CVE-2021-1643	CVE-2021-1672	CVE-2021-1713
CVE-2021-1644	CVE-2021-1676	CVE-2021-1714
CVE-2021-1645	CVE-2021-1677	CVE-2021-1715
CVE-2021-1647	CVE-2021-1694	CVE-2021-1716
CVE-2021-1648	CVE-2021-1696	CVE-2021-1725
CVE-2021-1656	CVE-2021-1699	

Vulnerabilidades adicionales informadas:

CVE-2021-1638	CVE-2021-1666	CVE-2021-1691
CVE-2021-1641	CVE-2021-1667	CVE-2021-1692
CVE-2021-1642	CVE-2021-1668	CVE-2021-1693
CVE-2021-1646	CVE-2021-1671	CVE-2021-1695
CVE-2021-1649	CVE-2021-1673	CVE-2021-1697
CVE-2021-1650	CVE-2021-1674	CVE-2021-1700
CVE-2021-1651	CVE-2021-1678	CVE-2021-1701
CVE-2021-1652	CVE-2021-1679	CVE-2021-1702
CVE-2021-1653	CVE-2021-1680	CVE-2021-1703
CVE-2021-1654	CVE-2021-1681	CVE-2021-1704
CVE-2021-1655	CVE-2021-1682	CVE-2021-1705
CVE-2021-1657	CVE-2021-1683	CVE-2021-1706
CVE-2021-1658	CVE-2021-1684	CVE-2021-1709
CVE-2021-1659	CVE-2021-1685	CVE-2021-1710
CVE-2021-1660	CVE-2021-1686	CVE-2021-1712
CVE-2021-1661	CVE-2021-1687	CVE-2021-1717
CVE-2021-1662	CVE-2021-1688	CVE-2021-1718
CVE-2021-1664	CVE-2021-1689	CVE-2021-1719
CVE-2021-1665	CVE-2021-1690	CVE-2021-1723

Fabricante

Microsoft

Productos afectados

ASP.NET Core 3.1
ASP.NET Core 5.0
Bot Framework SDK for .NET Framework
Bot Framework SDK for JavaScript
Bot Framework SDK for Python
Excel Services
HEVC Video Extensions
Microsoft 365 Apps for Enterprise (para sistemas 32-bit y 64-bit)
Microsoft Azure Kubernetes Service

Microsoft Edge (EdgeHTML-based)
Microsoft Excel
2010 Service Pack 2 (32-bit y 64-bit)
2013 RT Service Pack 1
2013 Service Pack 2 (32-bit y 64-bit)
2016 (32-bit y 64-bit)
Microsoft Office
2010 Service Pack 2 (32-bit y 64-bit editions)
2013 RT Service Pack 1
2013 (32-bit y 64-bit editions)
2016 (32-bit y 64-bit editions)
2019 (32-bit y 64-bit editions)
2019 for Mac
Online Server
Web Apps 2010 Service Pack 2
Web Apps 2013 Service Pack 1
Microsoft Remote Desktop
Microsoft Remote Desktop for Android
Microsoft Security Essentials
Microsoft SharePoint
Enterprise Server 2013 Service Pack 1
Enterprise Server 2016
Foundation 2010 Service Pack 2
Foundation 2013 Service Pack 1
Server 2010 Service Pack 2
Server 2019
Microsoft SQL Server
2012 for 32-bit Systems Service Pack 4 (QFE)
2012 for x64-based Systems Service Pack 4 (QFE)
2014 Service Pack 3 for 32-bit Systems (CU 4)
2014 Service Pack 3 for 32-bit Systems (GDR)
2014 Service Pack 3 for x64-based Systems (CU 4)
2014 Service Pack 3 for x64-based Systems (GDR)
2016 for x64-based Systems Service Pack 2 (GDR)
2016 Service Pack 2 for x64-based Systems (CU 15)
2017 for x64-based Systems (CU 22)
2017 for x64-based Systems (GDR)
2019 for x64-based Systems (CU 8)
2019 for x64-based Systems (GDR)
Microsoft System Center
2012 Endpoint Protection
2012 R2 Endpoint Protection
Endpoint Protection
Microsoft Visual Studio
2015 Update 3
2017 version 15.9 (includes 15.0 – 15.8)
2019 version 16.0
2019 version 16.4 (includes 16.0 – 16.3)
2019 version 16.7 (includes 16.0 – 16.6)
2019 version 16.8
Microsoft Word
2010 Service Pack 2 (32-bit y 64-bit editions)

2013 RT Service Pack 1 2013 Service Pack 1 (32-bit y 64-bit editions) 2016 (32-bit y 64-bit editions) Remote Desktop client for Windows Desktop Windows 10 (32-bit y 64-bit) Version 1607, 1803, 1809, 1909, 2004, 20H2, para 32 bit, 64 bit y ARM64-based Windows 7 32-bit Systems Service Pack 1 x64-based Systems Service Pack 1 Windows 8.1 32-bit systems x64-based systems Windows Defender Windows RT 8.1 Windows Server 2008 32-bit Systems Service Pack 2 32-bit Systems Service Pack 2 (Server Core installation) x64-based Systems Service Pack 2 x64-based Systems Service Pack 2 (Server Core installation) R2 for x64-based Systems Service Pack 1 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 2012 Server Core installation R2 y R2 (Server Core installation) Windows Server 2016 2016 Server Core installation Windows Server 2019 2019 Server Core installation Windows Server version 1909 (Server Core installation) version 2004 (Server Core installation) version 20H2 (Server Core installation)
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00361-01/
https://www.csirt.gob.cl/media/2021/01/9VSA21-00360-01.pdf

CSIRT comparte vulnerabilidades entregadas por Joomla	
Alerta de seguridad cibernética	9VSA21-00362-01
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 2021
Última revisión	13 de Enero de 2021
CVE	
CVE-2021-23123 - CVE-2021-23124 - CVE-2021-23125	
Fabricante	
Joomla	
Productos afectados	
Joomla! CMS desde la versión 3.0.0 hasta la 3.9.23. Joomla! CMS desde la versión 3.9.0 hasta la 3.9.23. Joomla! CMS desde la versión 3.1.0 hasta la 3.9.23.	
Enlaces para revisar el informe:	
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00362-01/	
https://www.csirt.gob.cl/media/2021/01/9VSA21-00362-01.pdf	

CSIRT comparte vulnerabilidades que afectan a Red Hat Quay	
Alerta de seguridad cibernética	9VSA21-00363-01
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 2021
Última revisión	13 de Enero de 2021
CVE	
CVE-2020-27831 - CVE-2020-3899 - CVE-2020-9802 CVE-2020-9327 - CVE-2020-8492 - CVE-2020-7595 CVE-2020-6405 - CVE-2020-3902 - CVE-2020-3901 CVE-2020-3900 - CVE-2020-3897 - CVE-2020-9805 CVE-2020-3895 - CVE-2020-3894 - CVE-2020-3885 CVE-2020-3868 - CVE-2020-3867 - CVE-2020-3865 CVE-2020-3864 - CVE-2020-3862 - CVE-2020-9803 CVE-2020-9806 - CVE-2020-1752 - CVE-2020-11793 CVE-2020-24659 - CVE-2020-15503 - CVE-2020-14422 CVE-2020-14391 - CVE-2020-14382 - CVE-2020-13632 CVE-2020-13631 - CVE-2020-13630 - CVE-2020-10029 CVE-2020-9807 - CVE-2020-10018 - CVE-2020-9925 CVE-2020-9915 - CVE-2020-9895 - CVE-2020-9894 CVE-2020-9893 - CVE-2020-9862 - CVE-2020-9850 CVE-2020-9843 - CVE-2020-1971 - CVE-2020-1751 CVE-2020-27832 - CVE-2019-8782 - CVE-2019-8816 CVE-2019-8815 - CVE-2019-8814 - CVE-2019-8813 CVE-2019-8812 - CVE-2019-8811 - CVE-2019-8808 CVE-2019-8783 - CVE-2019-8771 - CVE-2019-8820	

CVE-2019-8769 - CVE-2019-8766 - CVE-2019-8764 CVE-2019-8743 - CVE-2019-8720 - CVE-2019-8710 CVE-2019-8625 - CVE-2019-5018 - CVE-2018-20843 CVE-2019-8819 - CVE-2019-8823 - CVE-2020-1730 CVE-2019-19906 - CVE-2019-20916 - CVE-2019-20907 CVE-2019-20807 - CVE-2019-20454 - CVE-2019-20388 CVE-2019-20387 - CVE-2019-20218 - CVE-2019-19956 CVE-2019-19221 - CVE-2019-8835 - CVE-2019-16935 CVE-2019-16168 - CVE-2019-15903 - CVE-2019-15165 CVE-2019-14889 - CVE-2019-13627 - CVE-2019-13050 CVE-2019-8846 - CVE-2019-8844
Fabricante
Red Hat
Productos afectados
Joomla! CMS desde la versión 3.0.0 hasta la 3.9.23. Joomla! CMS desde la versión 3.9.0 hasta la 3.9.23. Joomla! CMS desde la versión 3.1.0 hasta la 3.9.23.
Enlaces para revisar el informe:
https://www.csirt.gob.cl/vulnerabilidades/9vsa21-00362-01-2/
https://www.csirt.gob.cl/media/2021/01/9VSA21-00363-01.pdf

IoC - Malware

A continuación, se comparten los Indicadores de Compromisos que fueron detectados durante la semana pasada por el Equipo del CSIRT.
CSIRT recomienda a los administradores y usuarios bloquear los hash publicados en este informe, y mantener un permanente monitoreo sobre el resto de los Indicadores de Compromiso.

Hash de archivos maliciosos

9c3a55f232d16099aefb638734d0bf5e3cfc1d353511cc940b8bc78eb8eade43
edccbee11901bbab7e53ce56b3f91ded2ebfe855f0529e9af035bf02926f23d7
af82c606594a45a22ee92b565a0f660c5747e865b42b2bff0c8f54973c6430a5
75da0babaec2dc03b34b3ac5a3a1d29befb6e45edcf9e079af9150416df63df4
f41191d034c431b657fe3879db9d982768d93e77fff9ba0cae2f7aa6de52a6e6

Correos electrónicos de donde son enviados los archivos adjunto con malware

vcalzolari64@tim.it
eva@hkshengpin.com
chad@greaterdimensions.com
marketing@aruj.com.pk

Direcciones IP de servidor SMTP donde es enviado el correo malicioso

82.57.200.98
82.57.200.99
69.12.73.228
82.57.200.100
203.128.6.25

IoC - Ataques de Fuerza Bruta

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

IP
77.88.224.66
144.217.199.2

Actualidad

Ciberconsejos para protegerse de los fraudes de verano

Cada vez son más las personas que arriendan alguna propiedad para sus vacaciones de verano a través de un sitio web. Sin embargo, así como incrementa esta tendencia también aparecen los avisos falsos que buscan obtener un beneficio económico.

Ver más: https://www.csirt.gob.cl/recomendaciones/ciberconsejos-para-protegerse-de-los-fraudes-de-verano/

Recomendaciones y Buenas Prácticas

Recomendaciones generales de seguridad

- 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 públicos 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 (en el sitio web https://www.csirt.gob.cl y/o al teléfono +(562) 2486 3850) siempre que hayan aportado con información relevante, manteniendo la reserva del incidente durante el análisis y hasta la certificación de la solución del mismo.

- Catalina Martínez
- Diego Neipan
- Rodrigo Cortés
- José Ávila
- Javier Martínez
- Boris López

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.01.15 15:54:02 -03'00'