



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática

BOLETÍN DE CIBERSEGURIDAD

Año 5 | N.º 254

semana del 10 al 16 de mayo de 2024

LA SEMANA EN CIFRAS

PARCHES COMPARTIDOS

86


Las mitigaciones son útiles en productos de Google Chrome, SAP y Microsoft.



CONTENIDO

1. Vulnerabilidades.....	3
2. Noticias y concientización.....	7
3. Recomendaciones y buenas prácticas	9
4. Muro de la Fama	10

1. Vulnerabilidades




Alerta de Vulnerabilidades

Google Chrome

CSIRT

Detalles e informe en <https://csirt.gob.cl/alertas>

Google Chrome - Vulnerabilidades	
Código de alerta	VSA24-01014
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de mayo de 2024
Última revisión	14 de mayo de 2024
CVE, puntaje EPSS al momento de la publicación	
CVE-2024-4761	0.04%
CVE-2024-4671	1.97%
Fabricante	
Google	
Productos afectados	
Google Chrome 124	
Enlaces para revisar el informe:	
https://csirt.gob.cl/alertas/vsa24-01014/	



Alerta de Vulnerabilidades





SAP Security Patch Day Mayo 2024

CSIRT

Detalles e informe en <https://csirt.gob.cl/alertas>

SAP Security Patch Day Mayo 2024 - Vulnerabilidades	
Código de alerta	VSA24-01015
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2024
Última revisión	16 de mayo de 2024
CVE y puntaje CVSS al momento de la publicación	
CVE-2019-17495	9.8
CVE-2024-33006	9.6
CVE-2022-36364	8.8
CVE-2024-28165	8.1
CVE-2024-32730	6.5
CVE-2024-34687	6.5
CVE-2024-32733	6.1
CVE-2024-33002	6.1
CVE-2024-32731	5.5
CVE-2024-33008	4.9
CVE-2024-33004	4.3
CVE-2024-33009	3.7
CVE-2024-33000	3.5
CVE-2024-33007	3.5
Fabricante	
SAP	
Productos afectados	
SAP Business Client HY_COM 2205	
SAP NetWeaver Application Server ABAP and ABAP Platform	
SAP BusinessObjects (Business Intelligence Platform) 430, 440	
SAP Enable Now 1704	
SAP S/4HANA (Manage Catalog Items and Cross-Catalog search)	
SAP Process Integration	

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

SAP Replication Server SAP S/4 HANA (Manage Bank Statement Reprocessing Rules) SAP BusinessObjects Business Intelligence Platform (Webservices) SAP Global Label Management (GLM)
Enlaces para revisar el informe:
https://csirt.gob.cl/alertas/vsa24-01015



Detalles e informe en <https://csirt.gob.cl/alertas>





Microsoft Update Tuesday 2024 Mayo - Vulnerabilidades

Código de alerta	VSA24-01016
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de mayo de 2024
Última revisión	16 de mayo de 2024

CVE y CVSS al momento de la publicación

CVE-2024-29994	7.8
CVE-2024-28902	5.5
CVE-2024-28900	5.5
CVE-2024-26238	7.8
CVE-2024-26217	5.5
CVE-2024-26211	7.8
CVE-2024-26207	5.5
CVE-2024-23593	6.7
CVE-2024-30020	8.1
CVE-2024-30019	6.5
CVE-2024-30018	7.8
CVE-2024-30017	8.8
CVE-2024-30016	5.5
CVE-2024-30015	7.5
CVE-2024-30014	7.5
CVE-2024-30012	6.8
CVE-2024-30011	6.5
CVE-2024-30010	8.8
CVE-2024-30009	8.8
CVE-2024-30008	5.5
CVE-2024-30007	8.8
CVE-2024-30006	8.8
CVE-2024-30005	6.8
CVE-2024-30004	6.8
CVE-2024-30003	6.8
CVE-2024-30002	6.8
CVE-2024-30001	6.8
CVE-2024-30000	6.8
CVE-2024-29999	6.8
CVE-2024-29998	6.8
CVE-2024-4761	
CVE-2024-32004	8.1
CVE-2024-32002	9.0
CVE-2024-30059	6.1
CVE-2024-30055	5.4
CVE-2024-30054	6.5
CVE-2024-30053	6.5
CVE-2024-30051	7.8

CONTACTO Y REDES SOCIALES CSIRT

-  <https://www.csirt.gob.cl>
-  Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
-  [@csirtgob](https://twitter.com/csirtgob)
-  <https://www.linkedin.com/company/csirt-gob>

Boletín de Ciberseguridad N° 254

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile



BOLETÍN 13BCS24-00263-01 | Semana del 10 al 16 de mayo de 2024

CVE-2024-30050	5.4
CVE-2024-30049	7.8
CVE-2024-30048	7.6
CVE-2024-30047	7.6
CVE-2024-30046	5.9
CVE-2024-30045	6.3
CVE-2024-30044	7.2
CVE-2024-30043	6.5
CVE-2024-30042	7.8
CVE-2024-30041	5.4
CVE-2024-30040	8.8
CVE-2024-30039	5.5
CVE-2024-30038	7.8
CVE-2024-30037	7.5
CVE-2024-30036	6.5
CVE-2024-30035	7.8
CVE-2024-30034	5.5
CVE-2024-30033	7.0
CVE-2024-30032	7.8
CVE-2024-30031	7.8
CVE-2024-30030	7.8
CVE-2024-30029	7.5
CVE-2024-30028	7.8
CVE-2024-30027	7.8
CVE-2024-30025	7.8
CVE-2024-30024	7.5
CVE-2024-30023	7.5
CVE-2024-30022	7.5
CVE-2024-30021	6.8
CVE-2024-29997	6.8
CVE-2024-29996	7.8





Fabricante

Microsoft

Productos afectados

Windows MSHTML Platform
Microsoft Office Excel
Windows DWM Core Library
Visual Studio
Microsoft Brokering File System
Windows Deployment Services
.NET and Visual Studio
Windows Kernel
Windows Cryptographic Services
Microsoft Intune
Windows CNG Key Isolation Service
Windows Cloud Files Mini Filter Driver
Windows Task Scheduler
Microsoft Windows SCSI Class System File
Microsoft Office SharePoint
Windows DHCP Server
Power BI
Microsoft Windows Search Component
Microsoft Bing
Windows Mobile Broadband
Windows Common Log File System Driver

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

Boletín de Ciberseguridad N° 254

Equipo de Respuesta ante Incidentes de Seguridad Informática | CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile







BOLETÍN 13BCS24-00263-01 | Semana del 10 al 16 de mayo de 2024

Windows Hyper-V
Windows Secure Boot
Azure Migrate
Windows Remote Access Connection Manager
Windows Win32K - GRFX
Microsoft WDAC OLE DB provider for SQL
Windows Win32K - ICOMP
Microsoft Edge (Chromium-based)
Microsoft Dynamics 365 Customer Insights
Windows Routing and Remote Access Service (RRAS)
Windows Mark of the Web (MOTW)
Windows NTFS

Enlaces para revisar el informe:

<https://csirt.gob.cl/alertas/vsa24-01016>

CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

2. Noticias y concientización

Ciberconsejos para un email más seguro

Esta semana les compartimos algunas recomendaciones básicas para estar más seguros al momento de usar nuestros correos electrónicos. Se tratan principalmente de revisar bien el remitente cuando nos llegue un email, no descargar todos los archivos que recibamos, ni tampoco hacer clic en enlaces, a menos que estemos convencidos de que son seguros.

Finalmente, compartimos también consejos para crear contraseñas más difíciles de adivinar por parte de los delincuentes. ¡Revisalos y compártelos! La campaña completa, para descargar y compartir con sus trabajadores, amigos y familiares, aquí:

<https://ciberseguridad.gob.cl/ciberconsejos/ciberconsejos-email-seguro/>.



CIBERCONSEJOS
CORREOS ELECTRÓNICOS:
PRINCIPALES MALAS PRÁCTICAS Y CÓMO CORREGIRLAS

CSIRT
Coordinación Nacional de Ciberseguridad
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

- ✗ No verificar el remitente**
 - ✓ Revisa que el remitente sea alguien que conozcas. Si el remitente te parece raro o imita una institución real, pero con errores, descártalo. Ojo, que el emisor aparezca como un remitente conocido no es garantía total de que se trate de un correo legítimo.
 - ✓ Sospecha de cualquier correo no solicitado.
 - ✓ Desconfía especialmente de correos con enlaces o archivos que se te indique descargar.

Ejemplo de email con remitente falso:

CUENTA SUSPENDIDA
BancoEstado <noreply@publmailier.com>
Para [Redacted]
Estimado(a):
BancoEstado su clave de Internet a vencido Su cuenta se encuentra S
- ✗ Hacer clic en cualquier enlace**
 - ✓ Evita hacer clic en enlaces que no estés seguro de que provienen de una fuente de confianza, y que de verdad necesitas abrir.
 - ✓ Si crees que pueda tratarse de un enlace importante, contáctate llamando a la persona o institución respectiva, o revisa tu cuenta escribiendo su URL directamente en la barra de direcciones.

Ejemplo de link malicioso disfrazado de PDF:

Factura no pagada, Marzo - 2024
CGE La Compañía General de Electricidad. <support@bvgo.ni>
Para [Redacted]
CGE La Compañía G
Hola, [Redacted]
Retraso en pago de factura - Regularización!
Accede a continuación para descargar tu factura vencida
PDF - Factura CGE - Chile (CGE-MARZO-2024 - 1 pags.)
- ✗ Abrir o descargar cualquier archivo**
 - ✓ Sólo descarga o abre archivos que estés realmente convencido no son un malware.

Ejemplo de email con mensaje urgente y adjunto malicioso:

Entrega urgente por DHL
Mensaje <mensaje@lovablehn.com>
Para [Redacted]
DHL_734825514200.rar
624 KB

CONTACTO Y REDES SOCIALES CSIRT

<https://www.csirt.gob.cl>
Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
@csirtgob
<https://www.linkedin.com/company/csirt-gob>

Exitosa cuarta versión de conferencia 8.8 Gobierno evidencia avances y desafíos del sector público en ciberseguridad

La actividad, que se llevó a cabo el 8 de mayo en el auditorio del Edificio Bicentenario, dio cuenta del interés de los encargados y equipos de ciberseguridad de los organismos públicos por avanzar en la materia y estar mejor preparados para enfrentar los retos que impone las amenazas y vulnerabilidades del mundo digital.

Daniel Álvarez Valenzuela, Coordinador Nacional de Ciberseguridad, abrió la jornada haciendo un recorrido por los avances en materia de ciberseguridad, destacando el hito del 8 de abril recién pasado, cuando se promulgó la Ley Marco de Ciberseguridad que crea un estándar regulatorio y una completa institucionalidad representada por la Agencia Nacional de Ciberseguridad (ANCI). Álvarez sostuvo que “Una de las primeras medidas relevantes es la obligatoriedad de notificar los incidentes de seguridad a todos los servicios esenciales, lo que nos va a permitir tener un completo mapa de amenazas y una visión mucho más precisa de los riesgos”.





“La capacitación, concientización y trabajo colaborativo son fundamentales en la ciberseguridad, ya que permite tener equipos preparados para saber cómo actuar frente a las distintas amenazas, además de generar planes de acción para prevenir o remediar un incidente de ciberseguridad. Y es este objetivo el que buscamos con la 8.8 Gobierno. Esta es la cuarta vez que realizamos este evento, que nos permite entregarle una visión global de las amenazas a los equipos de ciberseguridad y TI del Estado, actualizar conocimientos y fortalecer lazos”, enfatizó Cristian Bravo, Director del CSIRT de Gobierno.

La nota completa: <https://ciberseguridad.gob.cl/noticias/exitosa-cuarta-versi%C3%B3n-de-conferencia-88-gobierno-evidencia-avances-y-desaf%3ADos-del-sector-p%C3%ABlico-en-ciberseguridad/>

La jornada en video: <https://www.youtube.com/watch?v=ycl1T2XXC38>



CONTACTO Y REDES SOCIALES CSIRT

 <https://www.csirt.gob.cl>
 Teléfonos: 1510 | + (562) 24863850 | Correo: incidentes@interior.gob.cl
 @csirtgob
 <https://www.linkedin.com/company/csirt-gob>

3. 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.

CONTACTO Y REDES SOCIALES CSIRT

4. 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.

- Pablo Pizarro Cortinez
- Orlando Navarrete
- Andres Felipe Barrientos Cisternas
- Eduardo Arancibia
- Jaime Uribe
- Jorge Urrutia Müller
- Miguel Becerra

CONTACTO Y REDES SOCIALES CSIRT