Nro. Alerta:	EC-2022-53	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	28-marzo-2022	**Actualización de Google para parchear vulnerabilidad de día cero.**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Alto

II. ALERTA

Google Chrome publicó una solución de emergencia para el exploit de vulnerabilidad CVE-2022-1096.

Figura 1. Ilustración representativa de Google Chrome
Fuente: Google

III. INTRODUCCIÓN

El navegador Google Chrome creado por la compañía Google INC es uno de los navegadores que brinda mayor comodidad[1] a la hora de navegar por la web. Este navegador puede ser instalado en diferentes sistemas operativos y está disponible en más de 50 idiomas.

[1] La rapidez de Google Chrome se basa en la capacidad que tiene el navegador de procesar códigos de JavaScript.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-53	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	28-marzo-2022	**Actualización de Google para parchear vulnerabilidad de día cero.**	Versión 1.0

En este año, el gigante tecnológico; ha dado conocer una serie de vulnerabilidades que afectan al navegador. En este sentido; a través de CVE-2022-1096 se dio a conocer una vulnerabilidad de día cero de alta gravedad.

Como medida de mitigación, Google Chrome implementó actualizaciones automáticas de su navegador. Cabe señalar que la actualización a la versión 99.0.4844.84 estuvo disponible de inmediato al momento de realizar la presente alerta.

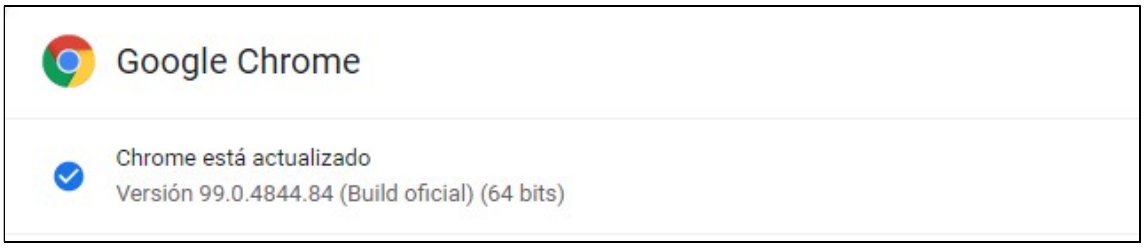

Figura 2. Actualización disponible de Google Chrome
Fuente: Propia

Con esta actualización, Google busca mitigar otra vulnerabilidad registrada como CVE-2022-0609; cabe señalar que el Grupo de Análisis de Amenazas de Google (TAG) dio a conocer que dos grupos de atacantes buscan explotar esta vulnerabilidad de RCE.

Estos dos grupos que buscan explotar la vulnerabilidad CVE-2022-0609, según al Informe de Threat Analysis Group; son respaldados por el gobierno de Corea del Norte y emplean el mismo kit de explotación con objetivos y técnicas diferentes. En la siguiente tabla se describen características de los atacantes.

		Nombre de Ciberdelincuentes	
No.	**Parámetro**	Operation Dream Job	Operation AppleJeus
1	**Descripción**	Orientada a más de 250 personas, que trabajan: • Medios de Comunicación. • Proveedores de alojamiento web. • Proveedores de software.	Orientada a más de 85 personas, que trabajan: • Industrias de criptomonedas. • Fintech.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-53	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	28-marzo-2022	**Actualización de Google para parchear vulnerabilidad de día cero.**	Versión 1.0

		Nombre de Ciberdelincuentes	
No.	**Parámetro**	Operation Dream Job	Operation AppleJeus
2	**Vector de Ataque**	Phishing • Recibían Correos supuestamente de reclutadores laborales de Disney, Google, Oracle. • A través de un click en el enlace adjunto en el correo, las víctimas recibían un iframe oculto que activa el kit de explotación.	Phishing • Creación de sitios web falsos para distribuir aplicaciones de criptomonedas troyanizadas. • Comprometer sitios web legítimos de empresas fintech y alojar iframes ocultos para entregar el kit de explotación a los visitantes.
3	**Dominios Falsos empleados**	disneycarreras[.]net encontrar-trabajo-de-sueño[.]com de hecho[.]org variedadtrabajo[.]com ziprecruiters[.]org	blockchainnoticias[.]vip cadenanoticias-estrella[.]com Financialtimes365[.]com bloques de fuego[.]vip fecha de caducidad[.]com gbclabs[.]com bloque gigante[.]org robot huming[.]io solonova[.]org
4	**KIT de explotación**	1. Los atacantes colocaron enlaces al kit de explotación dentro de iframes ocultos. 2. Emplea un script javascript que se usa para tomar huellas dactilares del sistema de destino. 3. Recopila la información y envía al C2. 4. Cumpliendo ciertas condiciones, la víctima recibe un exploit de Chrome RCE y algún javascript adicional.	

Tabla 3. Características grupos de atacantes vulnerabilidad CVE-2022-0609
Fuente: Threat Analysis Group

IV. VECTOR DE ATAQUE:

La vulnerabilidad corresponde a una debilidad de confusión de tipo de alta gravedad en el motor de JavaScript Chrome V8. Estas fallas de confusión de tipos, provocan fallas en el navegador luego de una explotación exitosa al leer o escribir memoria fuera de los límites del búfer.

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec

Nro. Alerta:	EC-2022-53	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	28-marzo-2022	**Actualización de Google para parchear vulnerabilidad de día cero.**	Versión 1.0

V. NOTA ACLARATORIA:

De momento Google no ha aportado más datos e indica que no lo hará hasta que considere controlado el problema.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Descargar programas y archivos de fuentes oficiales.
- Actualizar el navegador Google Chrome a la versión 99.0.4844.84 tanto para usuarios de Windows, Mac y Linux.
- A los usuarios de navegadores basados en Chromium, como Microsoft Edge, Opera y Vivaldi, se sugiere que apliquen las correcciones cuando estén disponibles.

VII. REFERENCIAS:

Adam, W. (27 de 03 de 2022). *Grupo de análisis de amenazas*. Obtenido de Grupo de análisis de amenazas: https://blog.google/threat-analysis-group/countering-threats-north-korea/

Conceptodefinicion. (05 de 02 de 2022). *Conceptodefinicion*. Obtenido de Conceptodefinicion: https://conceptodefinicion.de/google-chrome/

Gatlán, S. (25 de 03 de 2022). *BleepingComputer*. Obtenido de BleepingComputer: https://www.bleepingcomputer.com/news/security/emergency-google-chrome-update-fixes-zero-day-used-in-attacks/

Moreno, E. (28 de 03 de 202). *iTECHPOST*. Obtenido de iTECHPOST: https://www.itechpost.com/articles/109748/20220328/google-chrome-security-update-cve-2022-1096-high-severity-zero.htm

Paganini, P. (25 de 03 de 2022). *Securityaffairs*. Obtenido de Securityaffairs: https://securityaffairs.co/wordpress/129483/security/chrome-2nd-zero-day-2022.html

Dirección: Av. Amazonas N40-71 y Gaspar de Villaroel
Código postal: 170501 / Quito-Ecuador
Teléfono: 593-2 2271 180 - www.arcotel.gob.ec