Alerta de seguridad cibernética	9VSA21-00370-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	21 de enero de 2021
Última revisión	21 de enero de 2021

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Google, sobre vulnerabilidades que afectan a Google Chrome para escritorio.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

Vulnerabilidades

CVE-2021-21134
CVE-2021-21128
CVE-2021-21129
CVE-2021-21130
CVE-2021-21131
CVE-2021-21132
CVE-2021-21133
CVE-2021-21135
CVE-2021-21126
CVE-2021-21136
CVE-2021-21137
CVE-2021-21138
CVE-2021-21139
CVE-2021-21140
CVE-2021-21141
CVE-2021-21127
CVE-2021-21125
CVE-2021-21124
CVE-2021-21117
CVE-2021-21118
CVE-2021-21119
CVE-2021-21120
CVE-2021-21121
CVE-2021-21122
CVE-2021-21123
CVE-2020-16044

Impacto

Las vulnerabilidades de mayor riesgo son las siguientes:

Crítico:

CVE-2021-21117 permite a un atacante remoto evadir las restricciones de seguridad implementadas, debido a una aplicación insuficiente de las políticas en Cryptohome en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, evadir las medidas de seguridad implementadas y comprometer el sistema afectado.

Alto:

CVE-2021-21132 existe debido a una implementación incorrecta en DevTools en Google Chrome. Gracias a ella, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, y ganar acceso a información sensible.

CVE-2021-21135 permite a un atacante remoto acceder a información sensible, debido a una incorrecta implementación de la API de Performance en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, y ganar acceso a información sensible.

CVE-2021-22125 posibilita a un atacante remoto evadir las restricciones de seguridad implementadas, debido a un cumplimiento insuficiente de políticas en el API de Sistema de Archivos en Google Chrome. Por eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, evadir las medidas de seguridad implementadas y ganar acceso a información sensible.

CVE-2021-21124 existe a causa de un error de uso de memoria después de ser liberada dentro del componente de Reconocimiento de Voz en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo, lo que puede comprometer un sistema vulnerable.

CVE-2021-21118 ocurre debido a validación de datos insuficiente en V8.

CVE-2021-21123 se debe a una insuficiente validación de datos en la API del Sistema de Datos.

CVE-2021-21119 existe a causa de un error de uso de memoria después de ser liberada dentro del componente del componente Media en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo, lo que puede comprometer un sistema vulnerable.

CVE-2021-21120 existe a causa de un error de uso de memoria después de ser liberada dentro del componente del componente WebSQL en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo, lo que puede comprometer un sistema vulnerable.

CVE-2021-21121 existe a causa de un error de uso de memoria después de ser liberada dentro del componente del componente Omnibox en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo, lo que puede comprometer un sistema vulnerable.

CVE-2021-21122 existe a causa de un error de uso de memoria después de ser liberada dentro del componente del componente Blink en Google Chrome. Gracias a eso, un atacante remoto puede crear una página web especialmente diseñada, engañar a la víctima para que la visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo, lo que puede comprometer un sistema vulnerable.

CVE-2020-16044 tiene lugar debido a un error de uso de memoria después de ser liberada al procesar el trozo COOKIE-ECHO en un paquete SCTP. Un atacante remoto puede ingresar datos especialmente diseñados a un navegador, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema, pudiendo comprometer sistemas vulnerables.

Productos Afectados

Google Chrome, versiones de la 88.0.4324.0 a la 88.0.4324.95.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://chromereleases.googleblog.com/2021/01/stable-channel-update-for-desktop_19.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21134

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21128

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21129

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21130

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21131

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21132

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21133

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21135

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21126

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21136

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21137

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21138

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21139

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21140

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21141

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21127

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21125

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21124

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21117

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21118

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21119

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21120

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21121

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21122

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-21123

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-16044