Alerta de seguridad cibernética	9VSA21-00373-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de enero de 2021
Última revisión	25 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 Gentoo, sobre vulnerabilidades que afectan a Chromium y Google Chrome.

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

Vulnerabilidad

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

Impacto

Las vulnerabilidades de riesgo alto son las siguientes:

CVE-2020-16044: Permite a un atacante remoto comprometer sistemas vulnerables debido a un error de uso de memoria después de ser liberada al procesar COOKIE-ECHO en un paquete SCTP.

Un atacante remoto puede ingresar datos especialmente diseñados al navegador, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema.

CVE-2021-21117: Permite a un atacante remoto evadir las restricciones de seguridad implementadas, debido a un cumplimiento insuficiente de políticas en Cryptohome en Google Chrome.

Un atacante remoto puede engañar a la víctima para que visite un sitio especialmente diseñado, evadir las medidas de seguridad implementadas y comprometer al sistema afectado.

CVE-2021-21117: Permite a un atacante remoto evadir las restricciones de seguridad implementadas, debido a un cumplimiento insuficiente de políticas en la API File System en Google Chrome.

Un atacante remoto puede engañar a la víctima para que visite un sitio especialmente diseñado, evadir las medidas de seguridad implementadas y comprometer al sistema afectado.

CVE-2021-21119: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada dentro del componente Media de Google Chrome. Esto permite a un atacante remoto crear un sitio web y engañar a una víctima para que lo visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21120: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada dentro del componente WebSQL de Google Chrome. Esto permite a un atacante remoto crear un sitio web y engañar a una víctima para que lo visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21121: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada dentro del componente Omnibox de Google Chrome. Esto permite a un atacante remoto crear un sitio web y engañar a una víctima para que lo visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21122: Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada dentro del componente Omnibox de Google Chrome. Esto permite a un atacante remoto crear un sitio web y engañar a una víctima para que lo visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

CVE-2021-21124 Esta vulnerabilidad existe debido a un error de uso de memoria después de ser liberada dentro del componente de Reconocimiento de Voz de Google Chrome. Esto permite a un

atacante remoto crear un sitio web y engañar a una víctima para que lo visite, detonando un error de uso de memoria después de ser liberada y ejecutar código arbitrario en el sistema objetivo.

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

CVE-2021-21135: Esta vulnerabilidad existe debido a una implementación incorrecta en la API Performance en Google Chrome. Un atacante remoto puede crear una página especialmente diseñada, engañar a la víctima para que la visite y ganar acceso a información sensible.

Productos afectados

Chromium y Google Chrome, versiones anteriores a 88.0.4324.96.

Mitigación

Instalar las actualizaciones desde el sitio del proveedor.

Enlaces

https://security.gentoo.org/glsa/202101-13

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

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-2021-21124

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

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

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

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-2021-21134

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

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