Alerta de seguridad informática	9VSA20-00160-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	20 de marzo de 2020
Última revisión	20 de marzo de 2020

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 información obtenida de Google referente a múltiples vulnerabilidades que afectan a su navegador Google Chrome, las cuales de ser explotadas, permitirían a un atacante remoto comprometer completamente al sistema afectado. Este informe incluye la respectiva mitigación.

Vulnerabilidades

CVE-2020-6422

CVE-2020-6424

CVE-2020-6425

CVE-2020-6426

CVE-2020-6427

CVE-2020-6428

CVE-2020-6429

CVE-2020-6449

CVE-2019-20503

Impactos

CVE-2020-6422

Debido a un error en memoria (use-after-free) con WebGL en el explorador, un atacante remoto podría crear un sitio web malicioso para que la víctima lo visite, gatille el error en memoria y pueda ejecutar comandos arbitrarios en el sistema afectado. Esto le permitiría al atacante comprometer completamente al sistema.

CVE-2020-6424

Debido a un error en memoria (use-after-free) con un componente de media en el explorador, un atacante remoto podría crear un sitio web malicioso para que la víctima lo visite, gatille el error en memoria y pueda ejecutar comandos arbitrarios en el sistema afectado. Esto le permitiría al atacante comprometer completamente al sistema.

CVE-2020-6425

Debido a una insuficiente aplicación de políticas en las extensiones del explorador, un atacante podría engañar a una víctima para que instale una extensión maliciosa y ejecutar código arbitrario con privilegios elevados en el sistema afectado.

CVE-2020-6426

Debido a una incorrecta implementación del motor V8 en el explorador, un atacante remoto podría crear un sitio web malicioso para que la víctima lo visite y este pueda ejecutar comandos arbitrarios en el sistema afectado. Esto le permitiría al atacante comprometer completamente al sistema.

CVE-2020-6427, CVE-2020-6428, CVE-2020-6429, CVE-2020-6449

Debido a un error en memoria (use-after-free) con el componente de audio en el explorador, un atacante remoto podría crear un sitio web malicioso para que la víctima lo visite, gatille el error en memoria y pueda ejecutar comandos arbitrarios en el sistema afectado. Esto le permitiría al atacante comprometer completamente al sistema.

CVE-2019-20503

Debido a un error en memoria en “sctp_load_addresses_from_init” en “usrsctp”, un atacante podría entregarle datos especialmente diseñados a la aplicación, causar un error de lectura fuera de los límites de la memoria y acceder a contenidos en memoria no autorizados.

Producto Afectado

Google Chrome desde la versión 80.0.3987.0 hasta la 80.0.3987.148.

Mitigación

Actualizar a la versión 80.0.3987.149 de Google Chrome.

Enlaces

https://chromereleases.googleblog.com/2020/03/stable-channel-update-for-desktop_18.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6422
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6424
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6425
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6426
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6427
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6428
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6429
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-6449
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-20503

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.20 22:18:07 -03'00'