Alerta de seguridad cibernética	9VSA20-00316-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de noviembre de 2020
Última revisión	03 de noviembre 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 la información obtenida de múltiples fuentes respecto a vulnerabilidad que afecta al controlador criptográfico del Kernel de Windows y está actualmente siendo explotada. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-17087

Impacto

Esta vulnerabilidad podría permitir a un atacante realizar la escalación de privilegios en un sistema Windows. Además se ha descubierto que esta vulnerabilidad se encuentra siendo explotada junto con el CVE-2020-15999 (9VSA20-00312-01) de Google Chrome.
El controlador afectado "cng.sys" realiza un truncamiento incorrecto de enteros de 15 bits que provoca un desbordamiento de memoria intermedia. Esto podría permitir que un software malicioso o atacante en el sistema afectado pudiese explotar el fallo para lograr elevar sus privilegios y obtener acceso de administrador en los equipos comprometidos.

Productos Afectados

Windows 10 versión 2004
Windows 10 versión 1909
Windows 10 versión 1903
Windows 10 versión 1809
Windows 10 versión 1803
Windows 10 versión 1709
Windows 10 versión 1703
Windows 10 versión 1511
Windows 10 versión Gold
Windows 8
Windows 8.1
Windows 7 y Windows 7 SP1
Windows Server 2019 versión 2004
Windows Server 2019 versión 1909
Windows Server 2019 versión 1903
Windows Server 2019 versión 1803
Windows Server 2019 versión 1709
Windows Server 2016
Windows Server 2012 versión Gold
Windows Server 2012 versión R2
Windows Server 2008 versión R2 SP1
Windows Server 2008 versión SP2
Windows Server 2008 versión R2

Mitigación

Microsoft ha declarado que ya se encuentra trabajando en la solución. El martes 10 de noviembre se publicará en su ciclo habitual de parches.

Enlaces

https://www.cybersecurity-help.cz/vdb/SB2020103102
https://unaaldia.hispasec.com/2020/10/0-day-en-el-kernel-de-windows-esta-siendo-explotado-activamente.html
https://www.helpnetsecurity.com/2020/11/02/cve-2020-17087/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17087