Alerta de seguridad informática	9VSA20-00134-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	05 de febrero de 2020
Última revisión	05 de febrero 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 TeamViewer, referente a una vulnerabilidad que afecta su sistema de encriptación de contraseñas, la cual de ser explotada permitiría a un atacante local obtener las credenciales utilizadas en la aplicación. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-18988

Impacto

Teamviewer almacena las contraseñas de usuario cifradas con AES-128-CBC con la clave "0602000000a400005253413100040000" y con vector de inicialización "0100010067244F436E6762F25EA8D704" en el registro de Windows. Debido a esto un atacante local podría obtener las credenciales de la aplicación y obtener acceso a la máquina aun si Remote Desktop Protocol no se encuentra activo.
Además se presume que podría ser posible escalar a privilegios SYSTEM utilizando un archivo .bat.
Se hace un llamado a actualizar la aplicación apenas sean publicados los parches de seguridad.

Productos Afectados

Se presume que las versiones afectadas son las del año 2012 hasta la actual.

Mitigación

Aún no existe una manera de mitigar esta vulnerabilidad, TeamViewer se encuentra trabajando en ello, por lo que se hace un llamado a estar atento a las actualizaciones que sean publicadas.

Enlaces

https://community.teamviewer.com/t5/Announcements/Specification-on-CVE-2019-18988/m-p/82264
https://cve.mitre.org/cgi-bin/cvename.cgi?name= CVE-2019-18988

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.05 16:40:36 -03'00'