Nro. Alerta:	EC-2022-14	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	26-enero-2022	**Vulnerabilidad en TeamViewer en versiones anteriores a 15.21.2**	Versión 1.0

I. DATOS GENERALES:

Clase de alerta: Vulnerabilidad
Tipo de incidente: Sistema y/o Software Abierto
Nivel de riesgo: Bajo

II. ALERTA

TeamViewer en sus versiones anteriores a 15.21.2 presenta inconvenientes debido a la falta de una validación adecuada de los datos proporcionados por el usuario; dando espacio a que un usuario con pocos privilegios y haciendo uso de un código arbitrario; pueda revelar información del equipo afectado.

Figura 1.- Ilustración asociada a TeamViewer.
Fuente: TeamViewer

III. INTRODUCCIÓN

TeamViewer es un software que realiza un acceso remoto a un determinado equipo y otros dispositivos finales; permitiendo manejar a distancia dichos dispositivos; así mismo ofrece una variedad de funcionalidades, como acceder al sistema de archivos, tomar control del teclado e incluso el bloqueo de pantalla. Este proveedor de software a nivel mundial, cuenta con una gran cantidad de usuarios y un sin número de casos de éxitos en diferentes industrias como: Alimentos y bebidas, Software, Ciencia, Comercio, Finanzas, etc…

A pesar de ser una empresa con una vigencia superior a los 15 años; ha presentado diferentes vulnerabilidades en su producto; por ejemplo:

- En 2016 usuarios particulares y empresariales reportaron infecciones de ransomware.
- En 2020 una vulnerabilidad en TeamViewer permitía a un atacante robar contraseñas de manera remota y casi sin necesidad de interacción por parte del usuario, el CVE

Nro. Alerta:	EC-2022-14	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	26-enero-2022	**Vulnerabilidad en TeamViewer en versiones anteriores a 15.21.2**	Versión 1.0

asociado fue CVE 2020-13699.

- También los atacantes emplean esta plataforma para enviar anuncios fraudulentos en forma de ventanas emergentes que indican una infección en el equipo de la víctima y que incluyen un número de teléfono de un supuesto servicio técnico para solucionar el problema.

En este sentido, en el transcurso del presente año se asocia una nueva vulnerabilidad a TeamViewer; a continuación se mencionan características de esta vulnerabilidad:

Descripción	Detalle
Fecha de publicación de CVE	20 de enero de 2022.
Vulnerabilidad reportada al proveedor	18 de junio de 2021.
CVE asociado	CVE-2021-35005.
Versiones afectadas	Versiones anteriores a 15.21.2.
Puntuación CVSS	3.3

Tabla 1. Características generales de la vulnerabilidad.

IV. VECTOR DE ATAQUE: Local

La vulnerabilidad radica en una validación inadecuada de los datos proporcionados por el usuario; dando espacio a que un usuario con pocos privilegios pueda aprovechar esta situación para ejecutar un código arbitrario dentro del servicio de TeamViewer que se ejecuta como SISTEMA.; permitiendo revelar información confidencial sobre las instalaciones afectadas de TeamViewer.

V. IMPACTO

Existe cierta pérdida de confidencialidad originando que ciertos recursos dentro del componente afectado se divulguen al atacante; no hay pérdida de integridad ni de disponibilidad.

VI. RECOMENDACIONES:

El EcuCert recomienda a su comunidad objetivo:

- Actualizar TeamViewer a la versión v15.21.2 o superior disponible.
- Revisar periódicamente los boletines de seguridad emitidos por TeamViewer.

Nro. Alerta:	EC-2022-14	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS **ALERTA DE SEGURIDAD**	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS ECUCERT
TLP:	TLP:BLANCO		
Fecha:	26-enero-2022	**Vulnerabilidad en TeamViewer en versiones anteriores a 15.21.2**	Versión 1.0

VII. REFERENCIAS:

CVE.MITRE. (24 de 01 de 2022). *CVE.MITRE*. Obtenido de CVE.MITRE: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35005

NVD.NIST. (24 de 01 de 2022). *NVD.NIST*. Obtenido de NVD.NIST: https://nvd.nist.gov/vuln/detail/CVE-2021-35005

TeamViewer. (s.f.). *TeamViewer*. Obtenido de TeamViewer: https://www.teamviewer.com/es-mx/

TeamViewer. (s.f.). *TeamViewer*. Obtenido de https://teamviewer.uptodown.com/windows

Teamviewer, C. (20 de 01 de 2022). *Community Teamviewer*. Obtenido de Community Teamviewer: https://community.teamviewer.com/English/discussion/117794/august-updates-security-patches

Welivesecurity. (13 de 04 de 2021). *Welivesecurity*. Obtenido de Welivesecurity: https://www.welivesecurity.com/la-es/2021/04/13/teamviewer-riesgos-seguridad/#:~:text=En%202020%2C%20por%20ejemplo%2C%20TeamViewer,interacci%C3%B3n%20por%20parte%20del%20usuario.