BOLETÍN DE ALERTA

Boletín Nro.: 2021-30

Fecha de publicación: 16/11/2021

Tema: Múltiples vulnerabilidades en la plataforma Zoom.

Softwares afectados:

- **CVE-2021-34414**
  - Meeting Connector Controller hasta la versión 4.6.348.20201217.
  - Meeting Connector MMR hasta la versión 4.6.348.20201217.
  - Recording Connector hasta la versión 3.8.42.20200905.
  - Virtual Room Connector hasta la versión 4.4.6620.20201110.
  - Virtual Room Connector Load Balancer hasta la versión 2.5.5495.20210326.
- **CVE-2021-34415**
  - Meeting Connector Controller versiones anteriores a 4.6.358.20210205.
- **CVE-2021-34416**
  - Meeting Connector hasta la versión 4.6.360.20210325
  - Meeting Connector MMR hasta la versión 4.6.360.20210325
  - Recording Connector hasta la versión 3.8.44.20210326
  - Virtual Room Connector hasta la versión 4.4.6752.20210326
  - Virtual Room Connector Load Balancer hasta la versión 2.5.5495.20210326

Descripción:

Un grupo de investigadores ha identificado un total de tres fallos críticos que afectan a la plataforma Zoom, estos fallos pueden ser abusados por un administrador (o moderador) malintencionado del portal Zoom para inyectar y ejecutar comandos arbitrarios en la máquina que aloja el software.

A continuación se describen las vulnerabilidades:

CVE-2021-34414 de severidad alta con una puntuación de 7.2, se debe a que la página de proxy de red en el portal web para el controlador de Meeting Connector Controller, Meeting Connector MMR, Recording Connector, Virtual Room Connector y el Virtual Room

Connector Load Balancer no validan la entrada enviada en las solicitudes para actualizar la configuración del proxy de red, lo que podría llevar a la inyección de comandos remotos en el sistema local por un administrador del portal web.

CVE-2021-34415 de severidad alta con una puntuación de 7.5, se debe a que el servicio Zone Controller en Meeting Connector Controller, no verifica el campo cnt enviado en los paquetes de red entrantes, lo que conduce al agotamiento de los recursos y al bloqueo del sistema. Esta vulnerabilidad se eliminó en la versión 4.6.358.20210205 del Meeting Connector Controller.

CVE-2021-34416 de severidad crítica con una puntuación de 9.8, se debe a que el portal web de configuración administrativa de la dirección de red para Meeting Connector, Meeting Connector MMR, Recording Connector, Virtual Room Connector y Virtual Room Connector Load Balancer falla al validar la entrada enviada en las solicitudes para actualizar la configuración de red, lo que podría conducir a una inyección de comandos remotos en el sistema local por parte de los administradores del portal web.

Se debe tener en cuenta que todas estas vulnerabilidades se pueden explotar si un atacante logra obtener las credenciales de inicio de sesión de un usuario con derechos administrativos.

Impacto:

La explotación exitosa de las vulnerabilidades podría permitir a un atacante bloquear o secuestrar instancias locales del sistema de videoconferencia.

Solución:

Actualizar a la última versión disponible de las aplicaciones afectadas.

- Descargar la última versión disponible: https://zoom.us/download
- Actualizar a la última versión disponible: https://blogs.otago.ac.nz/zoom/how-to-update-zoom/

Información adicional:

- https://explore.zoom.us/en/trust/security/security-bulletin/
- https://www.ptsecurity.com/ww-en/about/news/positive-technologies-helps-eradicate-vulnerabilities-in-zoom/