Vulnerabilidad en microCLAUDIA (Broken Access Control)

From [redacted]

To incidentes@ccn-cert.cni.es

Date Monday, March 11th, 2024 at 5:54 PM

Buenos días,

Soy Alejandro Vázquez Vázquez (https://www.linkedin.com/in/vazquez-vazquez-alejandro/). Durante esta conferencia de Rooted tuve una charla con vuestro compañero Manuel, y hablamos sobre una vulnerabilidad existente en la herramienta microCLAUDIA, que descubrí al realizar algunas tareas diarias como miembro de un equipo de Telefónica que provee servicios para Amtega (Agencia para la Modernización Tecnológica de Galicia).

Quería ponerme en contacto con vosotros, como ya os han avisado, para comentaros el hallazgo y poder ayudar a su resolución.

Si recibís este correo, por favor contestadme y os envío la información que recopilé sobre la vulnerabilidad.

[CCN-CERT #[redacted] [AutoReply] Vulnerabilidad en microCLAUDIA (Broken Access Control)

From incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es>

To [redacted]

Date Monday, March 11th, 2024 at 5:55 PM

[English version below]

Estimado Sr./Sra.,

Este mensaje se ha generado automáticamente como respuesta a la creación de un ticket recibido relativo a: "**Vulnerabilidad en microCLAUDIA (Broken Access Control)**".

Se le ha asignado la referencia **[CCN-CERT #[redacted]** Por favor, inclúyala en la línea 'Asunto' de todos los mensajes relacionados con esta comunicación.

Gracias por la información. Si desea hacernos cualquier tipo de comentario o pregunta, o si necesita ayuda adicional, no dude en contactar con nosotros.

Atentamente,

Equipo CCN-CERT

Dear Mr./Ms.,

This message has been automatically generated in response to the creation of a ticket regarding: "**Vulnerabilidad en microCLAUDIA (Broken Access Control)**".

It has been assigned the reference number **[CCN-CERT #[redacted]** Please, include this reference in the 'Subject' line of any further messages dealing with this notification.

Thank you for reporting it. If you have any comments or questions, or if we can be of additional assistance, please let us know.

Best Regards,

CCN-CERT Team

==========

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre sistemas clasificados y sobre sistemas de las Administraciones Públicas y de empresas y organizaciones de interés estratégico para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

##############################
PGP key: incidentes@ccn-cert.cni.es
Fingerprint: 972B 04EC E24A 2C61 0E8D 1D4F C291 E8E1 348B ABEC
Download key from: https://www.ccn-cert.cni.es/documentos-publicos/1357-public-ccn-cert-incidentes/file.html
##################################

[CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es>

To [redacted]

Date Tuesday, March 12th, 2024 at 7:54 AM

Buenos días, Alejandro.

Estamos al tanto.

Puedes enviarnos la información cifrada con la clave PGP de incidentes:
[+] https://www.ccn-cert.cni.es/documentos-publicos/1357-public-ccn-cert-incidentes/file.html

O, si te parece, subirla a LORETO, nuestra nube privada:
[+] https://loreto.[redacted]

Gracias por tu colaboración.

Atentamente,
Equipo CCN-CERT.

CCN-CERT-INCIDENTES

Re: [CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From [redacted]

To incidentes@ccn-cert.cni.es

Date Wednesday, March 13th, 2024 at 11:33 AM

Buenos días,

Actualmente, tengo una carga de trabajo bastante elevada y no puedo ser tan ágil con este tema, como me gustaría. Os pido disculpas por adelantado.

En este correo, voy a resumir en definitiva lo que es la vulnerabilidad, pero ***me gustaría organizar una reunión*** con vosotros para verlo de forma conjunta y realizar una demostración en la que pueda detallar cada uno de los pasos de manera más clara.

Vulnerabilidad

[redacted]

Explotación

[redacted]

[redacted]

POC

Para facilitaros la detección y el hacer pruebas, [redacted]
detectar la presencia de esta vulnerabilidad (brokeclaudia_poc.zip). Nota: Solo os permite obtener información, tenéis que modificarlo si queréis apuntar a endpoints para [redacted]

Remediación

[redacted]

Referencias

[redacted]

Presentación

Como he señalado previamente, mi intención es convocar una sesión conjunta, una vez analicéis estos datos, donde pueda presentaros el fallo desde mi perspectiva y llevar a cabo una demostración práctica. Igualmente, os adelanto una breve presentación en PowerPoint que elaboré hace unos meses, diseñada para exponer la vulnerabilidad de manera ejecutiva (brokeCLAUDIA_Presentation.pptx, brokeCLAUDIA_Presentation.pdf).

Demos

Entre hoy y mañana intentaré volver a grabar los videos de POC que tengo, esta vez comentándolos, para que podáis apreciar el alcance de este fallo.

NOTA: Por favor, contestad a este correo para saber que habéis recibido la información🙄.

On Tuesday, March 12th, 2024 at 7:54 AM, incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es> wrote:

> Buenos días, Alejandro.
>
> Estamos al tanto.
>
> Puedes enviarnos la información cifrada con la clave PGP de incidentes:
> [+] https://www.ccn-cert.cni.es/documentos-publicos/1357-public-ccn-cert-incidentes/file.html
>
> O, si te parece, subirla a LORETO, nuestra nube privada:
> [+] https://loreto.[redacted]
>
> Gracias por tu colaboración.
>
> Atentamente,
> Equipo CCN-CERT.
>
> CCN-CERT-INCIDENTES

2.37 MB 3 files attached

brokeclaudia_poc.zip 27.94 KB

brokeclaudia_presentation.zip 2.34 MB

[redacted] 3.44 KB

[CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es>

To [redacted]

Date Wednesday, March 13th, 2024 at 3:59 PM

Recibido, le echamos un vistazo.

Atentamente,
Equipo CCN-CERT.

CCN-CERT-INCIDENTES

Re: [CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From [redacted]

To incidentes@ccn-cert.cni.es

Date Thursday, March 14th, 2024 at 4:07 PM

Buenos días,

Me disponía a enviaros los videos que grabé explotando la vulnerabilidad, pero me he dado cuenta de que ya habéis identificado la raíz del problema y os encontráis en el proceso de resolución. Imagino, entonces, que los videos quizás ya no os son necesarios.

No obstante, quedo a la espera por si necesitáseis mi apoyo en cualquier aspecto.

Un saludo.

On Wednesday, March 13th, 2024 at 3:59 PM, incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es> wrote:

> Recibido, le echamos un vistazo.
>
> Atentamente,
> Equipo CCN-CERT.
>
> CCN-CERT-INCIDENTES

3.44 KB 1 file attached

[redacted] 3.44 KB

Re: [CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From [redacted]

To incidentes@ccn-cert.cni.es

Date Tuesday, March 19th, 2024 at 11:51 AM

Buenos días,

He observado que habéis incluido [redacted]

Sin embargo, puede que ocurran incidencias en la funcionalidad de la aplicación, ya que [redacted]

Un saludo.

NOTA: Por favor, contestad a este correo para saber que habéis recibido la información🙂.

On Thursday, March 14th, 2024 at 4:07 PM,
wrote:

> Buenos días,
>
> Me disponía a enviaros los videos que grabé explotando la vulnerabilidad, pero me he dado cuenta de que ya habéis identificado la raíz del problema y os encontráis en el proceso de resolución. Imagino, entonces, que los videos quizás ya no os son necesarios.
>
> No obstante, quedo a la espera por si necesitáseis mi apoyo en cualquier aspecto.
>
> Un saludo.
>
> On Wednesday, March 13th, 2024 at 3:59 PM, incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es> wrote:
>
> > Recibido, le echamos un vistazo.
> >
> > Atentamente,
> > Equipo CCN-CERT.
> >
> > CCN-CERT-INCIDENTES

[CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es>

To [redacted]

Date Tuesday, March 19th, 2024 at 3:26 PM

CCN-CERT-INCIDENTES

281 bytes 1 file attached

20240319.txt 281 bytes

Buenas tardes, Alejandro.

Gracias por enviarnos la información. El equipo de desarrollo ha procurado, en primer lugar, eliminar la vulnerabilidad. Como dices, el siguiente fallo es el que comentas y en el que se está trabajando para corregir.

Atentamente,
Equipo CCN-CERT.

Re: [CCN-CERT #[redacted] Re: Vulnerabilidad en microCLAUDIA (Broken Access Control)

From [redacted]

To incidentes@ccn-cert.cni.es

Date Tuesday, March 19th, 2024 at 3:30 PM

Buenas tardes,

Recibido, si necesitáis ayuda con ello contactadme.

Un saludo.

On Tuesday, March 19th, 2024 at 3:26 PM, incidentes@ccn-cert.cni.es <incidentes@ccn-cert.cni.es> wrote:

> CCN-CERT-INCIDENTES