VIRTUALIT®

Soluciones Virtuales e Infraestructura Tecnológica

CORPORACIÓN NACIONAL DE TELECOMUNICACIONES

Cnt

INFORME TÉCNICO: CORRECCION DE VULNERABILIDADES v2.0

Preparado por

Fabian Toapanta
ftoapanta@virtualit.com.ec

Diciembre, 2018

SOLUCIONES VIRTUALES E INFRAESTRUCTURA TECNOLOGICA VIRTUALIT S.A.

RUC: 1792018080001

Calle Gaspar Escalona N38-39 y Villalengua

Quito - Ecuador

Tel (593) 2 381 5950

www.virtualit.com.ec

CONTENIDO

1 Antecedentes

La Corporación Nacional de Telecomunicaciones CNT por intermedio del Ing. David Peña quien ocupa el cargo de Analista de Ingeniería Data Center , solicita un Informe de vulnerabilidades el mismo que es presentado por la Analista Valeria Coronel el 23 de Noviembre del 2018, mostrando el resultado del Ethical Hacking realizado al aplicativo https://smart.cntcloud.com, en el cual se validan las acciones correctivas de las vulnerabilidades halladas en el aplicativo, presentadas en el informe No. 028-JCTI-INFOTEC-SI-2018 proporcionado por Ing. David Peña.

2 Objetivos

- Diagnosticar las mejores soluciones para la corrección de las vulnerabilidades del aplicativo.
- Realizar la implantación de las soluciones en el entorno de producción de la Corporación Nacional de Telecomunicaciones CNT

3 Estado de vulnerabilidades

A continuación se muestra las vulnerabilidades mostradas en el informe No. 028-JCTI-INFOTEC-SI-2018 v2.0 proporcionado por Ing. David Peña.

ID	Vulnerabilidad/ Hallazgo	Descripción	CVSS	Criticidad
1	Formularios HTML vulnerables a CSRF	CSRF permite a un atacante engañar a la víctima con acceso no legítimos, logrando capturar información confidencial de acceso del usuario	4.3	Medio
2	Denegación de servicios Slow HTTP	Para este ataque se hace uso de las solicitudes HTTP GET para ocupar todas las conexiones http disponibles permitidas en un servidor web. Este ataque aprovecha una vulnerabilidad en los servidores web basados en subprocesos que esperan que se reciban los encabezados HTTP completos antes de liberar las conexiones. Esto crea una situación en la que un usuario malintencionado podría abrir varias conexiones en un	7.5	Alto

		servidor al iniciar una solicitud HTTP pero no la cierra lo que consume los recursos y provoca un Dos		
3	Directorios web navegables	Se encontró que directorios web navegables, lo que significa que puede ver el contenido del directorio. Estos directorios se pueden encontrar: https://smart.cntcloud.com/assets/* https://smart-cntcloud.com/public/*	5	Medio
4	Denegación de Servicio	El servidor Apache actual con versión 2.4.34, al enviar marcos de configuración grandes y continuos, un cliente puede ocupar una conexión, un hilo del servidor y el tiempo de CPU sin que el tiempo de espera de la conexión entre en vigencia.	4.3	Medio
5	Clickjacking	Clickjacking es un método que permite a un atacante usar múltiples capas trasparentes para engañar a un usuario a realizar un clic sobre un enlace o botón de una página distinta de la piensa que está realizando el clic. Esto permite secuestrar clics para redirigir al usuario a una página ilegitima o robar información.	4.3	Medio
6	Cookie sin bandera HttpOnly	HttpOnly es una bandera adicional incluida en la cabecera de respuesta HTTP Set-Cookie, el uso de esta bandera ayuda a mitigar el riesgo que scripts de lado del cliente accedan a la cookie. Si el navegador del lado del cliente detecto una cookie con la bandera HttpOnly, mientras que un script intenta leerla, el navegador retornara una cadena vacía como resultado.	5	Medio
7	Cookie sin bandera Secure	El indicador de seguridad es una opción que el servidor de aplicaciones puede configurar al enviar una nueva cookie al usuario dentro de una respuesta HTTP. El propósito del indicador de seguridad	5	Medio

		es evitar que las cookies no sean observadas por terceros no autorizados debido a la transmisión de la cookie en texto claro.		

4 Detalle de Soluciones de las vulnerabilidades

4.1 Formularios HTML vulnerables a CSRF.

Para proteger el portal contra ataques Cross-Site Request Forgery se procedió a la implementación de configuraciones y funcionalidades que se describen a continuación:

4.1.1 Creación e implementación de Token CSRF.

Un token es una firma cifrada que permite a nuestro aplicativo identificar al usuario. En cuanto a un token CSRF cuenta con el mismo objetivo sin embargo son implementados en las solicitudes de trasferencia, lo que requiere que cada solicitud realizada por el aplicativo deba poseer un argumento extra como se muestra a continuación:

Figura 1 Token CSRF

La generación de los Token CSRF se la realiza médiate el uso del método openssl_random_pseudo_bytes, el cual genera una cadena de bytes pseudo-aleatoria, con el número de bytes determinado por el parámetro y a esta cadena se aplica el método bin2hex que convierte datos binarios en su representación hexadecimal.

4.1.2 Protección contra vulnerabilidades XSS.

Se implementó formularios con campos cuyo tipo son definidos, como se puede observar en la Figura 2.

Figura 2

Además se usó la función htmlspecialchars propia de PHP, esto permite convertir entidades HTML en caracteres especiales e impedir que el navegador reconozca estas entidades como si fueran parte del sistema. A continuación se muestra un ejemplo del proceso.

Tabla 1. Uso de htmlspecialchars

Texto Ingresado por el usuario	<script>window.alert("Test");</script>
Texto que se guarda en la base de datos	<script>window.alert("Test");</script>

4.1.3 Cierre automático de sesión.

Se estableció un tiempo de vida máximo para las sesiones creadas en el aplicativo, esta configuración se la realizo en la parte del servidor.

4.2 Denegación de servicios Slow HTTP

Se implanto la directiva reqtimeout, esta directiva puede establecer varios tiempos de espera para recibir los encabezados de solicitud y el cuerpo de solicitud del cliente. Si el cliente no envía los encabezados o el cuerpo dentro del tiempo configurado, se envía un error 408 REQUEST TIME OUT.

```
<IfModule mod_reqtimeout.c>
  RequestReadTimeout header=20-40,MinRate=500 body=20,MinRate=500
</IfModule>
```

Figura 3 Implementación de Modulo ReqTimeOut

4.3 Directorios web navegables

Se implementó un sistema de configuración principal de apache mediante la directiva <Directory> y la implementación de < Virtual Host>.

```
<Directory "C:/xampp/htdocs/cnt/public/">
    Options -Indexes
</Directory>
```

Figura 4 Implementación de la directiva Directory

4.4 Denegación de Servicio

Actualización el servidor Apache a la versión 2.4.37 la cual soluciona el problema de vulnerabilidad en él envió de configuraciones grandes y continuas.

```
C:\cmder
λ C:\xampp\apache\bin\httpd -v
Server version: Apache/2.4.37 (Win32)
Apache Lounge VC15 Server built:   Oct 18
 2018 17:16:04
```

Figura 5 Versión de Apache implementada

4.5 Clickjacking

Se añadió en la cabecera de las respuestas HTTP el campo X-Frame-Options: SAMEORIGIN, X-Content-Type-Options: nosniff y X-XSS-Protection: 1;mode=block.

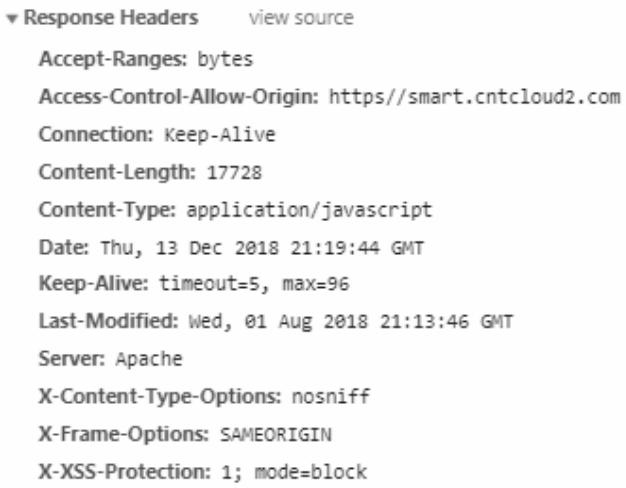

Figura 6 Respuesta de Header

4.6 Cookie sin bandera HttpOnly.

HttpOnly es una bandera adicional incluida en la cabecera de respuesta HTTP Set-Cookie, la misma fue implementada en las cookies utilizadas en el aplicativo.

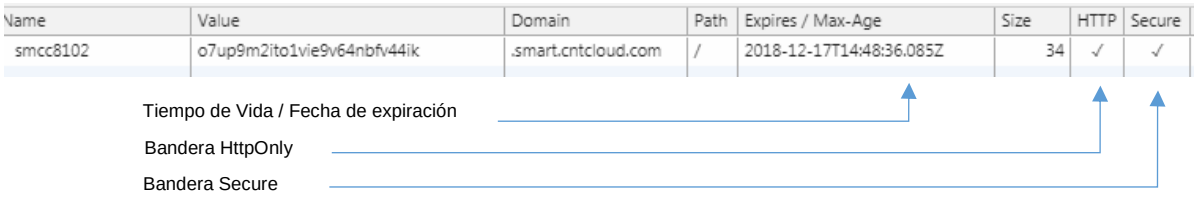

Figura 7 Propiedades de las Cookies en Google Chrome

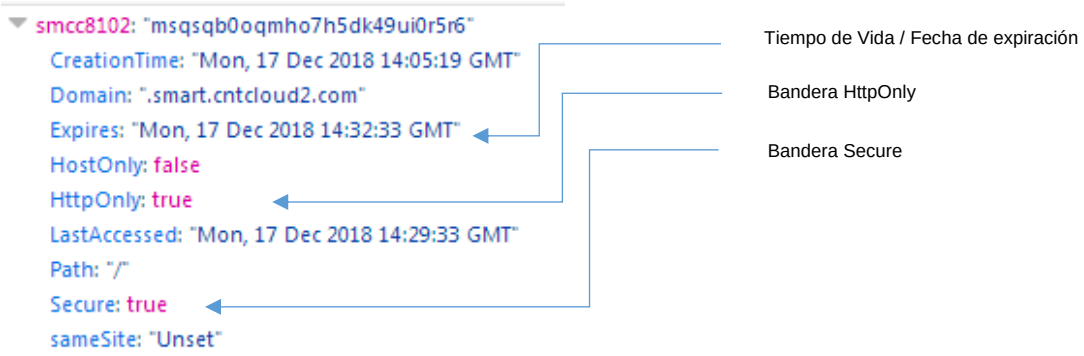

Figura 8 Propiedades de las Cookies en Firefox

4.7 Cookie sin bandera Secure.

El indicador de seguridad es una opción que el servidor de aplicaciones puede configurar al enviar una nueva cookie al usuario dentro de una respuesta HTTP ,esta opción fue implementada para las cookies del aplicativo como se muestra en la figura 7 & 8.

5 Conclusiones

- Se solucionaron las vulnerabilidades mostradas en el Informe presentado por la Corporación Nacional de Telecomunicaciones CNT.
- Se llevó a cabo la implementación de las soluciones de manera efectiva en colaboración con los encargados de Data Center virtual, en sesiones programadas por ambas partes.

6 Recomendaciones

- Se recomienda mantener actualizado el entorno de producción, tanto de parches de Sistema Operativo, como de los componentes del portal de aprovisionamiento.

7 Cláusula de Confidencialidad

La información expuesta en este documento es confidencial. Usted se compromete a adoptar medidas para prevenir la divulgación de la información como lo haría para impedir la divulgación de la información de su propiedad, usando en todos los casos un cuidado razonable.