VIRTUALIT

Soluciones Virtuales e Infraestructura Tecnológi

CORPORACIÓN NACIONAL DE TELECOMUNICACIONES

INFORME TÉCNICO: CORRECCION DE VULNERAVILIDADES

Preparado por

Fabian Toapanta
ftoapanta@virtualit.com.ec
Noviembre, 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 2
2 Objetivos 2
3 Estado de vulnerabilidades 2
4 Detalle de Soluciones de las vulnerabilidades 7
4.1 Usuario y contraseña de Tomcat por defecto. 7
4.2 Múltiples vulnerabilidades en Apache Tomcat 8
4.3 Fuga de información por scripts de Apache Tomcat 8
4.4 Autenticación básica HTTP habilitada 8
4.5 Método HTTP TRACE habilitado 8
4.6 El sujeto del certificado X.509 CN no coincide con el nombre de la entidad. 9
4.7 Servidor TLS/SSL admite sistemas de cifrado DES e IDEA 9
4.8 Directorios web navegables 9
4.9 Cliente Open SSL Dos debido al parámetro DH grande (CVE-2018-0732) 10
4.10 CLICKJACKING 10
4.11 Ejecución gratuita de código arbitrario en EXIF 10
5 Conclusiones 10
6 Recomendaciones 10
7 Cláusula de Confidencialidad 10

1 Antecedentes

La Corporación Nacional de Telecomunicaciones CNT por intermedio del Ing. Nicolas Ortiz, solicita un Informe de vulnerabilidades el mismo que es presentado por la Analista Valeria Coronel el 27 de septiembre del 2018, mostrando el resultado del Ethical Hacking realizado al aplicativo https://190.152.153.27/cnt/, en el cual se validan las vulnerabilidades que padece el portal y podría significar blancos de ataques y afecciones informáticas

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 entregado por la Corporación Nacional de Telecomunicaciones CNT.

N	Vulnerabilidad					Estado
1	Usuario y contraseña deTomcat por defecto	El usuario administrador del servicio Tomcat 'tomcat' tiene una contraseña por defecto. Como resultado, cualquier persona que tenga acceso al puerto Tomcat puede obtener acceso total a la máquina.	10	CRITICO	Las contraseñas por defecto son susceptibles a permitir acceso a los sistemas por lo que es necesario cambiar las contraseñas predeterminadas de las aplicaciones y aplicar criterios de credenciales robustas como lo dispone la normativa NIST 800-118	Corregido
2	Múltiples vulnerabilidades en Apache Tomcat	La versión del servicio Apache Tomcat está ve afectado por las siguientes vulnerabilidades: - Error de memoria en 'd1_both.c' relacionado con el manejo de paquetes DTLS que permite ataques de denegación de servicio. (CVE-2014-3505) - Error en 'd1_both.c' relacionado con el manejo de los mensajes DTLS que permite ataques de denegación de servicio debido a la gran cantidad de memoria que se consume. (CVE-2014-3506) - Error de pérdida de memoria en 'd1_both.c' relacionado con el manejo de paquetes DTLS especialmente diseñados que permiten ataques de denegación de servicio. (CVE-2014-3507)	7.5	ALTO	Actualizar la versión de Apache Tomcat a la versión más reciente.	Corregido

		- Error en la función 'OBJ_obj2txt' cuando se utilizan varias funciones de impresión 'X509_name_ *', que filtran los datos de la pila de proceso, lo que da como resultado la divulgación de información. (CVE-2014-3508) - Error relacionado con la 'extensión de formato de punto ec' manejo y clientes multiproceso que permite sobrescribir la memoria liberada durante una sesión reanudada. (CVE-2014-3509) - Error de referencia de referencia NULL relacionado con el manejo de suites anónimas de cifrado ECDH y mensajes que permiten ataques de denegación de servicio contra clientes. (CVE-2014-3510) - Error relacionado con el manejo de mensajes fragmentados de 'ClientHello' que permiten a un atacante de hombre en el medio forzar el uso de TLS 1.0, independientemente de los niveles de protocolo más altos admitidos tanto por el servidor como por el cliente. (CVE-2014-3511) - Errores de buffer overflow en 'srp_lib.c' relacionados con el manejo de los parámetros del protocolo de contraseña remota segura (SRP), que pueden permitir una denegación de servicio o tener otro impacto no especificado. (CVE-2014-3512) - Existe un problema de pérdida de memoria en 'd1_srtp.c' relacionado con el manejo de la extensión DTTP SRTP y mensajes de saludo especialmente diseñados que pueden permitir ataques de denegación de servicio. (CVE-2014-3513) - Error relacionado con la forma en que SSL 3.0 maneja los bytes de relleno al descifrar los mensajes cifrados utilizando cifras de bloque en el modo de encadenamiento de bloques de cifrado (CBC). Los atacantes de man in the middle pueden descifrar un byte seleccionado de un texto de cifrado en tan solo 256 intentos si pueden obligar a una aplicación víctima a enviar repetidamente los mismos datos a través de conexiones SSL 3.0 recién creadas. Esto también se conoce como el problema 'POODLE'. (CVE-2014-3566) - Existe un problema de pérdida de memoria en 't1_lib.c' relacionado con el manejo de tickets de sesión que puede permitir ataques de denegación de servicio. (CVE-2014-3567)				

		- Existe un error relacionado con el proceso de configuración de compilación y la opción de compilación 'no-ssl3' que permite a los servidores y clientes procesar mensajes inseguros de handshake SSL 3.0. (CVE-2014-3568) - Existe un error de eliminación de referencias de punteros NULL en 't1_lib.c', relacionado con el manejo de los mensajes ServerHello del protocolo de contraseña remota segura (SRP), que permite que un servidor malicioso bloquee un cliente, lo que genera una denegación de servicio. (CVE-2014-5139)				
		Además se presentan las siguientes vulnerabilidades altas, medias y críticas debido a la versión actual de Apache: – Apache Tomcat: Denegación de Servicio (CVE-2016-3092) – Apache Tomcat: Bajo: el filtro CORS tiene valores predeterminados inseguros (CVE-2018-8014) – Apache Tomcat: Ejecución remota de código (CVE-2016-8735) – Apache Tomcat: Ejecución remota de código (CVE-2017-12615) – Apache Tomcat: Ejecución remota de código (CVE-2017-12617) – Apache Tomcat: Bypass de seguridad (CVE-2016-0763) – Apache Tomcat: Bypass de seguridad (CVE-2016-0714) – Apache Tomcat: Divulgación de información (CVE-2016-6816) – Apache Tomcat: bajo: fijación de sesión (CVE-2015-5346) – Apache Tomcat: moderado: pérdida de token CSRF (CVE-2015-5351)				
3	Fuga de Información por scripts de Apache Tomcat	Los siguientes scripts de ejemplo que vienen con Apache Tomcat v4.x - v7.x pueden ser utilizados por los atacantes para obtener información sobre el sistema. También se sabe que estas secuencias de comandos son vulnerables a la inyección de scripts de sitios cruzados (XSS). /examples/jsp/num/numguess.jsp /examples/jsp/dates/date.jsp /examples/jsp/snp/snoop.jsp /examples/jsp/error/error.html	**7.8**	**ALTO**	Los scripts de ejemplo nunca deben instalarse en los servidores de producción.	Corregido

		/examples/jsp/sessions/carts.html /examples/jsp/checkbox/check.html /examples/jsp/colors/colors.html /examples/jsp/cal/login.html /examples/jsp/include/include.jsp /examples/jsp/forward/forward.jsp /examples/jsp/plugin/plugin.jsp /examples/jsp/jsptoserv/jsptoservlet.jsp /examples/jsp/simpletag/foo.jsp /examples/jsp/mail/sendmail.jsp / examples / servlet / HelloWorldExample / examples / servlet / RequestInfoExample / examples / servlet / RequestHeaderExample / examples / servlet / RequestParamExample / examples / servlet / CookieExample / examples / servlet / JndiServlet / examples / servlet / SessionExample /tomcat-docs/appdev/sample/web/hello.jsp				
4	Autenticación básica HTTP habilitada	El esquema de Autenticación Básica HTTP no se considera un método seguro de autenticación de usuario (a menos que se use junto con algún sistema seguro externo como TLS / SSL), ya que el nombre de usuario y la contraseña se transfieren a través de la red como texto sin formato. Aplica los siguientes enlaces: http://190.152.153.27:8080/manager/status http://190.152.153.27:8080/manager/html http://190.152.153.27:8080/host-manager/html http://localhost:8080/manager/text/undeploy?path=/examples http://localhost:8080/manager/text/stop?path=/examples http://localhost:8080/manager/text/start?path=/examples http://localhost:8080/manager/text/sessions?path=/examples http://localhost:8080/manager/text/serverinfo http://localhost:8080/manager/text/resources[?type=xxxxx] http://localhost:8080/manager/text/reload?path=/examples http://localhost:8080/manager/text/lis	**6.5**	**ALTO**	Habilite HTTPS en el servidor web. El protocolo TLS / SSL protegerá las credenciales de Autenticación básica de texto claro.	Corregido

		http://localhost:8080/manager/text/ADw-script AD4-alert(42) ADw-/ http://localhost:8080/manager/text/ADw-script AD4-alert(42) ADw- http://localhost:8080/manager/text/findleaks[?statusLine=[true|false]] http://localhost:8080/manager/text/ http://localhost:8080/manager/text/deploy?path=/foo http://localhost:8080/manager/text http://localhost:8080/manager/jmxproxy/ADw-script AD4-alert(42) ADw-/ http://localhost:8080/manager/jmxproxy/CVS/ http://localhost:8080/manager/jmxproxy/ADw-script AD4-alert(42) ADw- http://localhost:8080/manager/status http://localhost:8080/manager/jmxproxy/ http://localhost:8080/manager/html http://localhost:8080/host-manager/html http://190.152.153.27:8080/host-manager/html http://190.152.153.27:8080/host-manager/html http://190.152.153.27:8080/manager/html;jsessionid=6C4FC6A77545151951D8				
5	Método HTTP TRACE habilitado	El método HTTP TRACE se usa normalmente para devolver la solicitud HTTP completa al cliente solicitante para fines de depuración del proxy. Un atacante puede crear una página web usando XMLHTTP, ActiveX o XMLDOM para hacer que un cliente emita una solicitud TRACE y capture las cookies del cliente. Esto da como resultado un ataque Cross-Site Scripting.	**5**	**MEDIO**	Deshabilitar dichos métodos en el servidor	Corregido
6	El sujeto del certificado X.509 CN no coincide con el nombre de la entidad	El campo de nombre común (CN) del sujeto en el certificado X.509 no coincide con el nombre de la entidad que presenta el certificado. Antes de emitir un certificado, una Autoridad de Certificación (CA) debe verificar la identidad de la entidad que solicita el certificado, como se especifica en la Declaración de Prácticas de Certificación (CPS) de la CA. Por lo tanto, los procedimientos estándar de validación de certificados requieren que el campo CN sujeto de un certificado coincida con el nombre real de la entidad que presenta el certificado. Por ejemplo, en un certificado presentado por "https://www.example.com/", el CN debe ser www.example.com.	**7.1**	**ALTO**	El campo de nombre común (CN) del sujeto en el certificado X.509 se debe fijar para reflejar el nombre de la entidad que presenta el certificado (por ejemplo, el nombre de host). Esto se hace generando un nuevo certificado generalmente firmado por una Autoridad de Certificación (CA) en la que confían tanto el cliente como el servidor.	Corregido
7	Servidor TLS / SSL admite sistemas de cifrado DES e IDEA	El protocolo Transport Layer Security (TLS) versiones 1.0 (RFC 2246) y 1.1 (RFC 4346) incluyen conjuntos de cifrado basados en los algoritmos DES (Data Encryption Standard) e IDEA (International Data Encryption Algorithm). Los algoritmos DES e IDEA ya no se recomiendan para uso general en TLS, y se han eliminado de la versión 1.2 de TLS.	**5.8**	**MEDIO**	Configure el servidor para deshabilitar el soporte para los conjuntos de cifrado DES e IDEA.	Corregido

8	Directorios web navegables	Se encontró que directorios web navegables, lo que significa que cualquiera puede ver el contenido del directorio. Estos directorios se pueden encontrar: https://190.152.153.27/dashboard/ https://190.152.153.27/IMG/ https//190.152.153.27/dashboard/ http://190.152.153.27/IMG/	5	MEDIO	Asegurarse que los directorios expuestos no contengan información confidencial, restringir su acceso o deshabilitar la indexación para los directorios que lo hagan. Añadir al archivo de configuración principal de Apache las siguientes líneas y recargar el servicio: <Directory RUTA_DIRECTORIO> Options -Indexes </Directory>	Corregido
9	Cliente OpenSSL DoS debido al parámetro DH grande (CVE-2018-0732)	Durante el acuerdo de clave en un protocolo de enlace TLS utilizando un cifrado basado en DH (E), un servidor malicioso puede enviar un gran valor primordial al cliente. Esto causará que el cliente pase un período de tiempo irracionalmente largo generando una clave para este primo que resultará en un bloqueo hasta que el cliente haya terminado. Esto podría ser explotado en un ataque de denegación de servicio. Reparado en OpenSSL 1.1.0i-dev (Afectado 1.1.0-1.1.0h). Reparado en OpenSSL 1.0.2p-dev (Afectado 1.0.2-1.0.2o).	7.5	ALTO	Aplicar la versión más actual para OpenSSL	Corregido
10	CLICKJACKING	Clickjacking es un método que permite a un atacante usar múltiples capas transparentes 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 ilegítima o robar información.	4.3	MEDIO	Añadir en la respuesta de cabecera HTTP el campo X-Frame-Options: SAMEORIGIN, para indicar al navegador que restringa la visualización del sitio dentro un marco, asegurando que el contenido del sitio no pueda ser embebido en otros sitios.	Corregido
11	Ejecución gratuita de código arbitrario en EXIF	La versión de PHP que se ejecuta en el servidor web remoto se ve afectada por una vulnerabilidad de ejecución de código arbitrario Use-After-Free.	4.3	MEDIO	Actualice a PHP versión 7.2.8 o posterior.	Corregido

4 Detalle de Soluciones de las vulnerabilidades

4.1 Usuario y contraseña de Tomcat por defecto.

Se realizó el cambio de credenciales por defecto, la cual cuenta con el criterio de credenciales robustas como lo dispone la normativa NIST 800-118. Por otra parte la administración de credenciales estará a cargo de VirtualIT de forma confidencial.

4.2 Múltiples vulnerabilidades en Apache Tomcat

El servidor Apache Tomcat fue actualizado de la versión 7.0 a 9.0.12

Server Information	
Tomcat Version	JVM Version
Apache Tomcat/9.0.12	1.8.0_171-b11

Ilustración 1 Versión de Tomcat

4.3 Fuga de información por scripts de Apache Tomcat

Los scripts de ejemplo fueron removidos del servidor de producción.

Applications	
Path	Version
/InterfazGCnt	None specified
/manager	None specified

Ilustración 2 Aplicaciones disponibles en Tomcat

4.4 Autenticación básica HTTP habilitada

Se habilito Https en el servidor web Apache Tomcat.

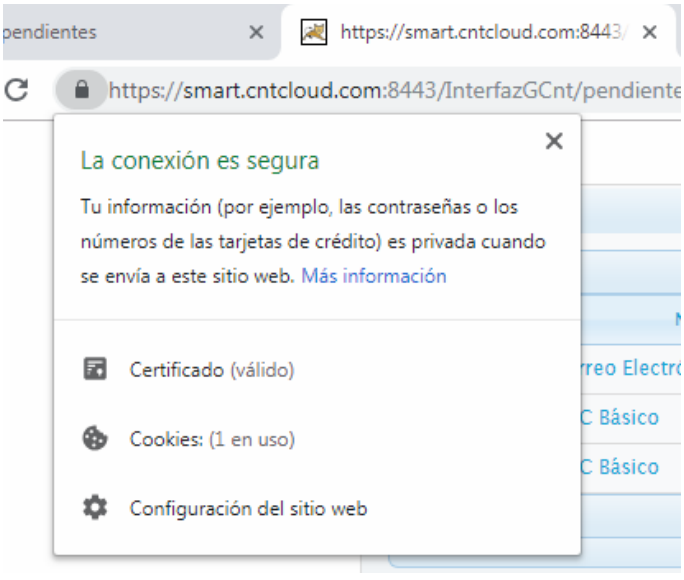


Ilustración 3 Https en aplicación Tomcat

4.5 Método HTTP TRACE habilitado

Método Trace deshabilitado.

4.6 El sujeto del certificado X.509 CN no coincide con el nombre de la entidad.

Certificados digitales generado por parte de la Corporación Nacional de Telecomunicaciones CNT.

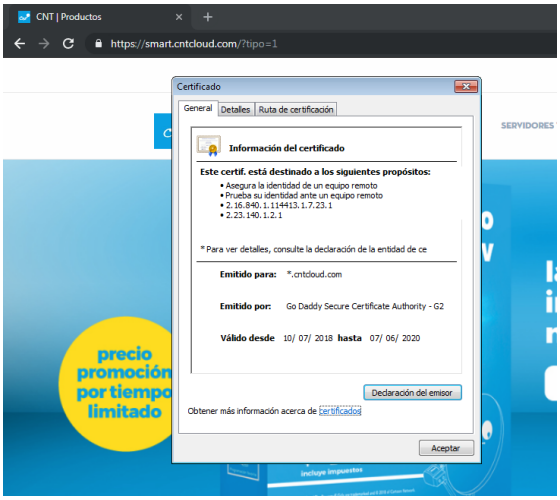


Ilustración 4 Certificado digital

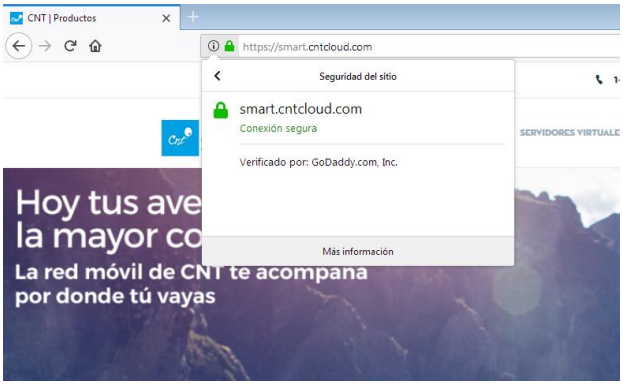


Ilustración 5 Conexión segura.

4.7 Servidor TLS/SSL admite sistemas de cifrado DES e IDEA

Se eliminó el soporte del protocolo Transport Layer Security versión 1.0 y 1.1

4.8 Directorios web navegables

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

```
<VirtualHost 190.152.153.27:443>
    <Directory "C:/xampp2/htdocs/cnt/">
        AllowOverride All
        Require all granted
    </Directory>
```

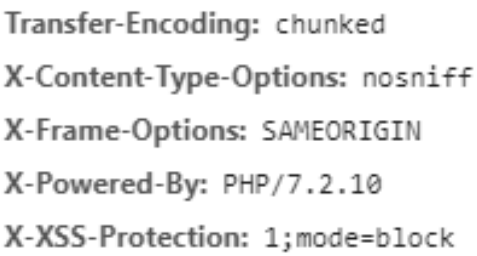
Ilustración 6 VirtualHost para el aplicativo smart.cntcloud.com

4.9 Cliente Open SSL Dos debido al parámetro DH grande (CVE-2018-0732)

Se actualizo Open SSL a la versión 1.1.0i

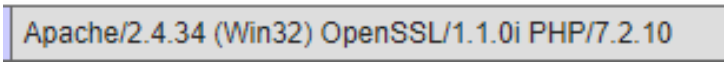
4.10 CLICKJACKING

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.



4.11 Ejecución gratuita de código arbitrario en EXIF

Se procedió a la actualización de PHP a la versión 7.10



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.