**Como proteger su servidor de la vulnerabilidad HTTProxy**

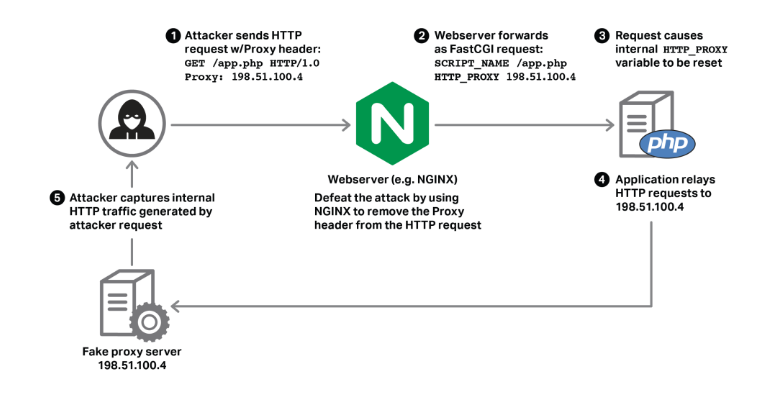
**problema publicado el día 18 de julio del 2016**

Por Diego Muses. Uruguay

Los servidores web utilizan la variable de entorno HTTP\_PROXY que permite especificar un servidor proxy (IP -URL- y puerto) para usarse de forma genérica desde la shell u otras aplicaciones como elinks, lynx, wget, curl, etc.

Por otro lado en CGI, según reza su [RFC 3875](https://tools.ietf.org/html/rfc3875#section-4.1.18), se añade automáticamente el meta tag "HTTP\_" para especificar el protocolo, por lo que si añadimos en la petición HTTP una cabecera "PROXY" probablemente sobrescribiremos la variable de entorno HTTP\_PROXY del servidor víctima, consiguiendo así especificar un proxy falso y facilitando un ataque MiTM (Man-in-the-Middle)

Cómo funciona el ataque.



Se puede ver más claro y ya de paso comprobar si el servidor es vulnerable fácilmente.   
  
Por ej. crear un sencillo script CGI:  
  
**test.cgi:  
#!/bin/sh echo "Content-Type:text/plain" ​echo "" echo "HTTP\_PROXY='$HTTP\_PROXY'"**  
  
y luego llamarlo con el header extra “Proxy:”  
  
**curl -H ‘Proxy: AFFECTED’ http://my-server-name/cgi-bin/test.cgi**   
Si la salida es HTTP\_PROXY='AFFECTED', estaría comprometido, así de sencillo.  
   
Este bug ya se identificó y parcheó en 2001 en perl y curl. Lo que pasa es que recientemente se está viendo que este fallo también existe en otros lenguajes y librerías, se le ha puesto el nombre 'httpoxy’, algunos CVEs que hacen referencia a los ambientes afectados son:

* CVE-2016-5385: PHP
* CVE-2016-5386: Go
* CVE-2016-5387: Apache HTTP Server
* CVE-2016-5388: Apache Tomcat
* CVE-2016-1000109: HHVM
* CVE-2016-1000110: Python

Mientras los parches no estén disponibles los administradores del servidores web con CGI deben bloquear la cabecera 'Proxy' si no quiere que du sistema empiece a usar un proxy malicioso.  
  
**Solución en Apache**  
Se debe cargar el modulo "mod\_headers" en la configuración y luego agregar una linea **"RequestHeaderunset Proxy early"**

**Centos y Fedora Core**

**vi /etc/httpd/conf/httpd.conf**   
Modulo necesario (descomentar)  
**LoadModuleheaders\_module modules/mod\_headers.so**  
  
Linea filtro encabezado proxy (agregar)  
**RequestHeaderunset Proxy early**

Verificamos configuración y reiniciamos el servicio

**>apachectl configtest**

**>service httpd restart**

**Ubuntu y Debian**  
**>sudo a2enmod headers  
>sudo vi /etc/apache2/apache2.conf**

agregar la línea

**RequestHeaderunset Proxy early**

Verificamos configuración y reiniciamos el servicio

**>sudo apache2ctl configtest**

**>sudo service apache2 restart**

También se puede filtrar con el módulo mod\_security agregando lo siguiente

**SecRuleEngine On**

**SecRule&REQUEST\_HEADERS:Proxy "@gt 0"**

**"id:1000005,log,deny,msg:'httpoxy denied'"**

**Microsoft ha proporcionado la siguiente guía para los servidores IIS que utilizan framework de terceros afectados**

Actualizar la configuración "apphost.config" con esta regla

**<system.webServer>**

**<rewrite>**

**<rules>**

**<rule name=3D"Erase HTTP\_PROXY" patternSyntax=3D"Wildcard">**

**<match url=3D"\*.\*" />**

**<serverVariables>**

**<set name=3D"HTTP\_PROXY" value=3D"" />**

**</serverVariables>**

**<action type=3D"None" />**

**</rule>**

**</rules>**

**</rewrite>**

**</system.webServer>**