

UNAM-CERT

Departamento de Seguridad en Cómputo

DGSCA-UNAM

Nota de Seguridad UNAM-CERT-2007-001

[Actualización] Ataques Phishing/Pharming Explotando Vulnerabilidades en Ruteadores 2Wire

En días pasados el UNAM-CERT y diversos Equipos de Respuesta a Incidentes de Seguridad en Cómputo han estado enterados de la propagación de correos electrónicos que utilizan técnicas de ataques Cross-site request forgery (XSRF) y Drive-by-pharming para tomar ventaja de una vulnerabilidad de autenticación en los ruteadores 2Wire y de esta forma redireccionar a los usuarios a sitios Web falsos de banca electrónica.

Fecha de Liberación: 7 de Diciembre de 2007

Ultima Revisión: 5 de Febrero de 2008

Fuente: UNAM-CERT

CVE ID: CVE-2007-4389

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Ejecución Remota de Código

I. Sistemas Afectados

- ◆ Ruteadores 2Wire proporcionando servicio independiente al sistema operativo.
- ◆ Los modelos donde se han realizado pruebas exitosas de la explotación de la vulnerabilidad son: 2700HG Gateway y 2701HG Gateway, aunque no se descarta que otros modelos sean vulnerables.

II. Descripción

Los ruteadores 2Wire distribuidos por diversos ISPs en México presentan una vulnerabilidad de autenticación que puede ser explotada por un atacante remoto no autenticado para ejecutar código arbitrario que le permita reiniciar el ruteador, cambiar la contraseña de la cuenta de administración del ruteador y de esta forma tomar inclusive el control completo del mismo.

UNAM-CERT

Hoy en día existen distintos vectores de ataques entre los que se encuentran la explotación a través de correos electrónicos de Phishing Scam, aunque estos pueden variar. El Proyecto Malware ha realizado el análisis de código malicioso contenido en este tipo de correos electrónico y ha realizado la publicación de los resultados obtenidos a través de su blog en:

- ◆ Proyecto Malware: Blog de Actividad Reciente de la Semana 49 –
<<http://www.malware.unam.mx/blog.dsc?semana=49>:

El UNAM-CERT ha desarrollado un documento técnico en el cual se detalla el proceso de ataque y pruebas de concepto de escenarios de explotación, el cual puede ser consultado en:

- ◆ Vulnerabilidad de autenticación en ruteadores 2Wire –
<<http://www.seguridad.unam.mx/doc/?ap=tutorial>

III. Impacto

La vulnerabilidad en los ruteadores 2Wire permite la ejecución remota de código dando como resultado que un intruso remoto no autenticado tome el control completo del equipo.

Es importante señalar que los vectores de ataque analizados hasta hoy se enfocan a realizar Pharming sobre los ruteadores 2Wire redireccionando al usuario a sitios Web falsos y cambiando la contraseña de administración del ruteador aunque en realidad el atacante tiene el control total del ruteador y podría ser capaz de realizar cualquier acción.

IV. Solución

◆ Actualización de seguridad

El fabricante ha liberado una actualización de seguridad que soluciona las vulnerabilidades existentes en ruteadores 2wire descritas en esta Nota de Seguridad liberada por UNAM-CERT el 7 de diciembre de 2007. La más severa de las vulnerabilidades, encontrada por UNAM-CERT, permitía la modificación de la configuración del ruteador aún si tenía una contraseña asignada, según se describe en el documento Vulnerabilidad de autenticación en ruteadores 2Wire del DSC/UNAM-CERT, y que estaba siendo utilizada para ataques de tipo Pharming.

UNAM-CERT conjuntamente con el equipo de ingeniería de Telmex han verificado y validado que la versión de firmware 5.29.135.5 corrige las vulnerabilidades conocidas para los ruteadores 2wire.

En México, para los usuarios de Prodigy Infinitum, Telmex ha confirmado que aplicará la actualización de seguridad de forma automática para los modelos 171HG, 1070, 1700HG, 2700, 2070 y 2701HG de ruteadores 2wire. Durante el mes de febrero el proveedor realizará el proceso de actualización a la versión 5.29.135.5 del firmware de los modelos de ruteadores 2wire mencionados. En la siguiente sección de ésta nota se describe el proceso para verificar la versión del firmware de los modem ruteador 2wire.

Telmex actualizará exclusivamente los modelos 171HG, 1070, 1700HG, 2700, 2070, 2701HG de ruteadores. Los usuarios de Prodigy Infinitum con un modelo distinto podrán solicitar al proveedor la actualización de sus dispositivos para poder contar con la actualización de seguridad correspondiente. El fabricante liberará un boletín relativo a esta actualización de seguridad.

UNAM-CERT

Si cuenta con un ruteador 2wire proporcionado por un ISP distinto a Telmex, por favor contacte a su Proveedor de Internet para obtener mayor información.

◆ ¿Cómo verifico la versión del firmware?

Para llevar a cabo la verificación de la versión actual del firmware con que cuenta el equipo 2wire, se debe realizar el siguiente procedimiento:

Abrir un navegador y escribir una de las siguientes URLs:

http://home/xslt?PAGE=A07_POSTTPAGE=A07

http://gateway.2wire.net/xslt?PAGE=A07_POSTTPAGE=A07

http://192.168.1.254/xslt?PAGE=A07_POSTTPAGE=A07

http://192.168.0.1/xslt?PAGE=A07_POSTTPAGE=A07

http://172.16.0.1/xslt?PAGE=A07_POSTTPAGE=A07

Al acceder a la URL, aparecerá una pantalla como la siguiente:

En esta pantalla, en el campo "Software version" (señalado en rojo en la imagen) contiene la versión del firmware y ésta debe ser mayor o igual a 5.29.135.5.

Si la versión para su ruteador 2wire es menor a la 5.29.135.5, el firmware no ha sido actualizado. En tal caso, deberá esperar a que se realice la actualización automática, o bien, ponerse en contacto con su Proveedor de Internet para solicitar mayor información al respecto.

◆ ¿Cómo verifico si mi ruteador está comprometido?

A continuación se enumeran los pasos que debes seguir para verificar si tu ruteador 2Wire ha sido comprometido:

1. Abre una ventana de tu navegador (puede ser Internet Explorer, Mozilla, etc.).
2. En la barra de dirección escribe o copia alguna de las siguientes direcciones (puede ser alguna de las siguientes dependiendo del modelo de tu ruteador):

http://192.168.1.254/xslt?PAGE=H04_POSTTPAGE=J38

http://192.168.0.1/xslt?PAGE=H04_POSTTPAGE=J38

http://home/xslt?PAGE=H04_POSTTPAGE=J38

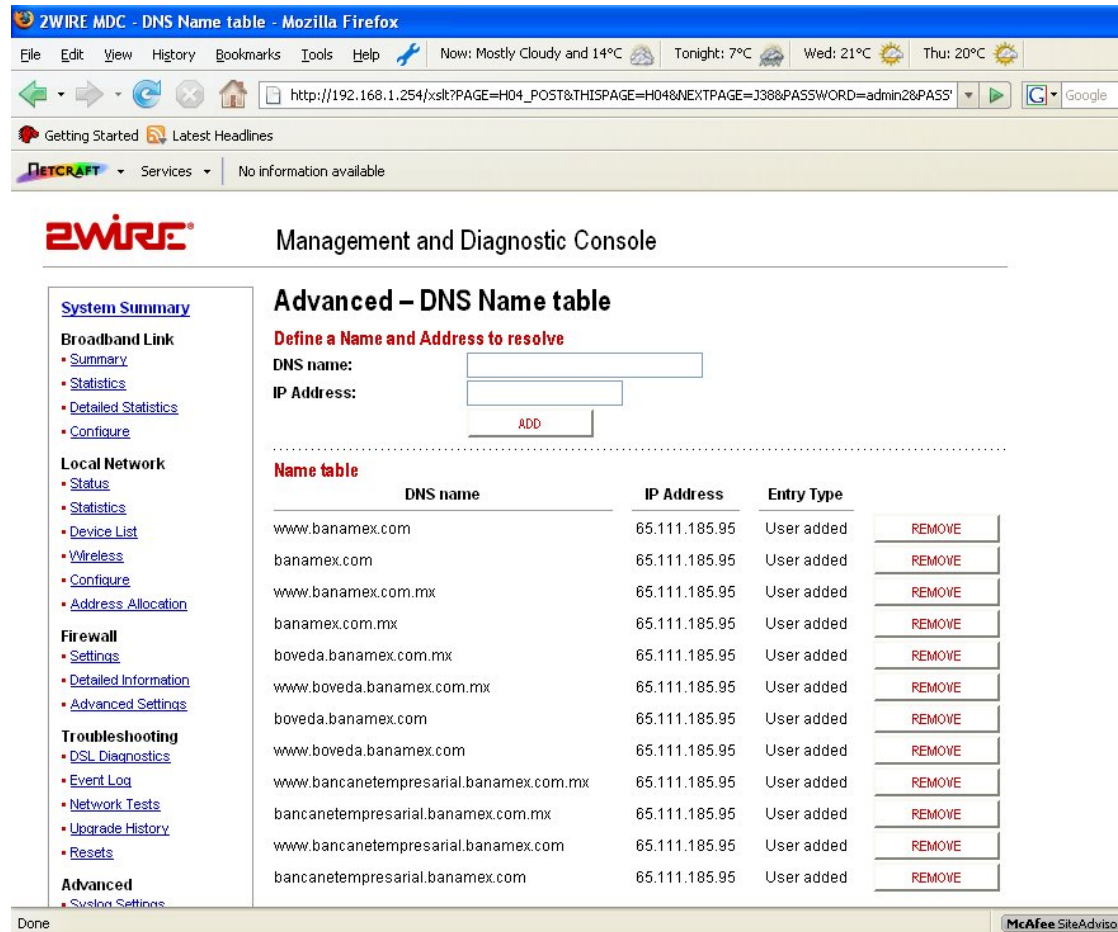
http://gateway.2wire.net/xslt?PAGE=H04_POSTTPAGE=J38

http://172.16.0.1/xslt?PAGE=H04_POSTTPAGE=J38

3. Si en la ventana de tu navegador se muestra un listado de direcciones IP asociadas a distintos dominios DNS (especialmente de banca electrónica) el ruteador muy probablemente ha sido comprometido.

UNAM-CERT

A continuación se muestra un ejemplo de lo que podrías visualizar en el caso de que tu router se encuentre comprometido:



The screenshot shows the 'Advanced - DNS Name table' configuration page in the 2Wire MDC Management and Diagnostic Console. The page includes a sidebar with navigation links for System Summary, Broadband Link, Local Network, Firewall, Troubleshooting, and Advanced. The main content area shows a form to 'Define a Name and Address to resolve' with fields for 'DNS name' and 'IP Address', and an 'ADD' button. Below the form is a table titled 'Name table' with columns for 'DNS name', 'IP Address', and 'Entry Type'. The table lists several entries, each with a 'REMOVE' button next to it.

DNS name	IP Address	Entry Type	
www.banamex.com	65.111.185.95	User added	REMOVE
banamex.com	65.111.185.95	User added	REMOVE
www.banamex.com.mx	65.111.185.95	User added	REMOVE
banamex.com.mx	65.111.185.95	User added	REMOVE
boveda.banamex.com.mx	65.111.185.95	User added	REMOVE
www.boveda.banamex.com.mx	65.111.185.95	User added	REMOVE
boveda.banamex.com	65.111.185.95	User added	REMOVE
www.boveda.banamex.com	65.111.185.95	User added	REMOVE
www.bancanetempresarial.banamex.com.mx	65.111.185.95	User added	REMOVE
bancanetempresarial.banamex.com.mx	65.111.185.95	User added	REMOVE
www.bancanetempresarial.banamex.com	65.111.185.95	User added	REMOVE
bancanetempresarial.banamex.com	65.111.185.95	User added	REMOVE

4. Para solucionar temporalmente el problema se deben eliminar manualmente los registros ingresados con el botón de “REMOVE”.

V. Referencias

- ◆ Vulnerabilidad de autenticación en routers 2Wire, DSC/UNAM-CERT <<http://www.seguridad.unam.mx/doc/?ap=tutorial>>
- ◆ Buenas prácticas de seguridad <<http://www.seguridad.unam.mx/usuario-casero/secciones/bpracticadsc>>
- ◆ Drive-By Pharming, Symantec – <http://www.symantec.com/avcenter/reference/Driveby_Pharming.pdf>
- ◆ 2Wire routers xslt cross-site request forgery – <<http://xforce.iss.net/xforce/xfdb/36044>>
- ◆ 2Wire Routers Cross-Site Request Forgery Vulnerability – <<http://secunia.com/advisories/26496>>
- ◆ Cross Site Request Forgery in 2Wire routers – <<http://www.securityfocus.com/archive/1/archive/1/476595/100/0/threaded>>
- ◆ Nuevo método de fraude bancario – <<http://blog.hispasec.com/laboratorio/255>>

El Departamento de Seguridad en Computo/UNAM-CERT agradece el apoyo en la traducción, elaboración y revisión de éste Documento a:

- Luis Fernando Fuentes Serrano (lfuentes at seguridad dot unam dot mx)

UNAM-CERT

- Ruben Aquino Luna (raqino at seguridad dot unam dot mx)
 - Eduardo Espina García (eespina at seguridad dot unam dot mx)
 - Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)
 - Juan Carlos Guel Lopez (cguel at seguridad dot unam dot mx)
-

UNAM-CERT

Equipo de Respuesta a Incidentes UNAM

Departamento de Seguridad en Cómputo

incidentes at seguridad.unam.mx

phishing at seguridad.unam.mx

http://www.cert.org.mx

http://www.seguridad.unam.mx

ftp://ftp.seguridad.unam.mx

Tel: 56 22 81 69

Fax: 56 22 80 43