UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−027

Negación de Servicio en Ruteadores 2Wire

En los últimos días el UNAM−CERT ha recibido reportes acerca de una vulnerabilidad existente en ruteadores 2Wire modelo 1701HG, 1800HW, 2071HG, 2700HG, 27001HGT, aunque no se descarta que la vulnerabilidad pueda existir en otros modelos. La explotación exitosa de la vulnerabilidad podría permitir a un atacante realizar ataques de negación de servicio (DoS).

Fecha de Liberación:	12 de Noviembre de 2008
Ultima Revisión:	18 de Noviembre de 2008
Fuente:	UNAM−CERT, foros y diversas listas de discusión.

Riesgo

Bajo

Problema de Vulnerabilidad

Local y remoto

Tipo de Vulnerabilidad

Negación de servicio

I. Sistemas Afectados

- El UNAM−CERT ha realizado pruebas exitosas sobre ruteadores modelo 2700 HG y 2701 HG−T, así como en las versiones de firmware 4.25.19, 5.29.51 y 5.29.52. Sin embargo, no se descarta la existencia de otros modelos 2Wire vulnerables.

II. Descripción

Existe una vulnerabilidad de negación de servicio a través del portal Web de diversos modelos de ruteadores 2Wire debido a que los valores pasados por la url no son debidamente validados. Un atacante podría explotar la vulnerabilidad enviando solicitudes a */xslt* al parámetro "page" con valores %X donde la "X" corresponde a cualquier caracter no alfanumérico. La explotación exitosa de la

vulnerabilidad sólo podría ocasionar una negación de servicio al lograr que la conexión DSL sea interrumpida y en algunas ocasiones podría causar que el dispositivo se reinicie.

Un atacante podría explotar la vulnerabilidad a través del envío de un archivo malicioso o convenciendo al usuario de que haga clic a un vínculo en una página html que contenga la liga malintencionda.

III. Impacto

Un atacante con acceso al sitio Web del ruteador podría ocasionar una negación de servicio temporal o permanente a través de valores construidos maliciosamente que sean enviados vía URL.

IV. Solución

Hasta el momento no existe solución oficial de la vulnerbilidad, sin embargo el UNAM−CERT recomienda lo siguiente:

- No habilitar la administración remota del dispositivo.
- No ejecutar ni abrir archivos de remitentes desconocidos o bien que pudieran contener potencialmente algún malware.

V. Referencias

- 2Wire Routers Denial of Service Vulnerability − http://secunia.com/advisories/32631/
- 2Wire Router DSL Denial of Service − http://milw0rm.com/exploits/7060
- Vulnerabilidad de Negación de Servicio en rutedores 2Wire − http://www.seguridad.unam.mx/doc/?ap=articulo

---

El Departamento de Seguridad en Cómputo/UNAM−CERT agradece el apoyo en la elaboración ó traducción y revisión de éste Documento a:

- Oscar Raúl Ortega Pacheco (oortega at seguridad dot unam dot mx)
- Eduardo Espina García (eespina at seguridad dot unam dot mx)
- Juan Carlos Guel Lopez (cguel at seguridad dot unam dot mx)
- Jorge Christian Durán Lara (bec_jduran 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 47