UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−017

Vulnerabilidad de evasión de Autenticación en SNMPv3

Una vulnerabilidad en la forma en que las implementaciones de SNMPv3 manejan paquetes creados especialmente podría permitir que se evada la autenticación en este protocolo.

Fecha de Liberación: 10 de Junio de 2008

Ultima Revisión: 16 de Junio de 2008

Fuente: US−CERT

CVE ID: **CVE−2008−0960**

Riesgo

Importante

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Validación inapropiada

I. Sistemas Afectados

Diversas implementaciones de SNMPv3

II. Descripción

El Protocolo de Administracion Simple de Redes (SNMP, por sus siglas en ingles) es un protocolo ampliamente difundido que se usa comunmente para monitorear y administrar dispositivos de red.

SNMPv3 (RFC 3410) soporta un modelo de seguridad basado en los usuarios (RFC 3414) que incorpora algunas características de seguridad como autenticación y control de privacidad. La autenticación por SNMPv3 se hace usando un código de autenticación de mensaje por hash (HMAC), un código de autenticación de mensajes que se calcula usando una función hash criptográfica en combinación con una llave privada.

Las implementaciones de SNMPv3 podrían permitir un código HMAC recortado en el campo de autenticación para validar a un agente o a un demonio usando un HMAC mínimo de 1 byte. El reducir HMAC a un byte significa hacer que un ataque de fuerza bruta se vuelva trivial.

Este problema se ha visto en Net−SNMP y UCD−SNMP. Puede ser que otras implementaciones de SNMP también se vean afectadas.

III. Impacto

Esta vulnerabilidad permite a los atacantes leer y modificar cualquier objeto SNMP que pueda ser accesado usando las credenciales que tienen en el sistema. Así mismo les permite ver y modificar la configuración de los dispositivos controlados. Los atacantes deben obtener acceso usando credenciales con privilegios de escritura para modificar configuraciones.

IV. Solución

Actualizar

Consulte al fabricante del dispositivo para obtener mayor mas información.

Aplicar un parche

Net−SNMP ha liberado un parche para resolver este problema. A los usuarios se les recomienda ampliamente aplicar este parche tan pronto como sea posible.

El parche debe de instalarse también de manera transparente a UCD−snmp.

Habilitar el subsistema de privacidad de SNMP3

La configuración debe de modificarse para habilitar el subsistema de privacidad de SNMPv3 para cifrar el tráfico de éste protocolo usando una llave privada, secreta.

Esta opción no cifra HMAC, pero minimiza la posibilidad de ser afectado por esta vulnerabilidad.

V. Referencias

- RFC 3410 − <http://tools.ietf.org/html/rfc3410>
- RFC 3414 − <http://tools.ietf.org/html/rfc3414>
- SECURITY RELEASE: Multiple Net−SNMP Versions Released − <http://sourceforge.net/forum/forum.php?forum_id=833770>

VI. US−CERT Vulnerability Note − <http://www.kb.cert.org/vuls/id/878044>

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

- Manuel I. Quintero Martínez (mquintero at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)

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