UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−004

El IOS de Cisco es afectado por diversas vulnerabilidades

El CERT/UNAM−CERT informa que se han descubierto diversas vulnerabilidades en el Internet Operating System (IOS) de Cisco. Un intruso remoto podría ejecutar código arbitrario en un dispositivo afectado, provocar que un dispositivo afectado recargue el sistema operativo o provocar otro tipo de negaciones de servicio.

Fecha de Liberación:	24 de Enero de 2007
Ultima Revisión:	25 de Enero de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Muy Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. **Sistemas Afectados**

Dispositivos de red de Cisco que ejecutan IOS en diversas configuraciones.

II. **Descripción**

Cisco ha publicado tres boletines de seguridad describiendo fallas en IOS con diferentes impactos de seguridad, el mas serio de ellos podría permitir a un atacante remoto ejecutar código arbitrario en el sistema afectado. Detalles adicionales están disponibles en las siguientes Notas de Vulnerabilidad:

VU#217912 − Cisco IOS falla al procesar adecuadamente paquetes TCP.

El demonio TCP de Cisco IOS en ciertas versiones del software Cisco IOS contiene una corrupción de memoria. Esta corrupción de memoria podría permitir a un atacante remoto crear una negación de servicio.

VU#341288 − Cisco IOS falla al procesar adecuadamente ciertos paquetes que contienen una opción IP modificada.

Existe una vulnerabilidad en la manera en que Cisco IOS procesa un número de paquetes IPv4 diferentes que contienen una opción IP modificada. Una explotación exitosa de esta vulnerabilidad podría permitir a un atacante, ejecutar código arbitrario en un dispositivo afectado o crear una negación de servicio.

VU#274760 − Cisco IOS falla al procesar adecuadamente paquetes IPv6 modificados.

Cisco IOS falla al procesar adecuadamente paquetes IPv6 con cabeceras de ruteo especialmente modificadas. Una explotación exitosa de esta vulnerabilidad podría permitir a un atacante ejecutar código arbitrario en un dispositivo afectado o crear una negación de servicio.

III. Impacto

Aunque el impacto de cada una de estas tres vulnerabilidades es un poco diferente, en el caso de las Notas de Vulnerabilidad VU#341288 y VU#274760, un atacante remoto podría causar la recarga del sistema operativo en un dispositivo afectado. En algunos casos, esto crea una situación de negación de servicio de forma secundaria, debido a que los paquetes no son reenviados a través del dispositivo afectado mientras este esta en el proceso de recarga. Explotaciones repetidas de estas vulnerabilidades podrían resultar en una negación de servicio prolongada.

Debido a que los dispositivos ejecutando IOS podrían transmitir trafico hacia otras redes, el impacto de una negación de servicio de forma secundaria sería severa.

Además en el acaso de las Notas de Vulnerabilidad VU#341288 y VU#274760, una explotación exitosa podría permitir a un atacante remoto la ejecución de código arbitrario en el dispositivo afectado.

IV. Solución

Actualizar a versión reciente de IOS

Cisco ha actualizado versiones del software IOS para corregir estas vulnerabilidades. Dirigirse a las secciones "Software Version and Fixes" del Aviso de Seguridad de Cisco listado en la sección de Referencias de este documento para obtener mayor información sobre la actualización.

Solución Temporal

Cisco también ha publicado soluciones temporales prácticas para estas Vulnerabilidades. Diríjase a la sección de "Soluciones Temporales" de cada

Aviso de Seguridad de Cisco listados en la sección de Referencias de este documento para mayor información.

Sitios que no puedan instalar una versión actualizada de OIS deben implementar estas soluciones temporales.

V. Referencias

* Nota de Vulnerabilidad UNAM−CERT VU#217912 − http://www.kb.cert.org/vuls/id/217912

* Nota de Vulnerabilidad UNAM−CERT VU#341288 − http://www.kb.cert.org/vuls/id/341288

* Nota de Vulnerabilidad UNAM−CERT VU#274760 − http://www.kb.cert.org/vuls/id/274760

* Aviso de Seguridad de Cisco: Paquetes TCP alterados pueden causar una Negación de Servicio − http://www.cisco.com/warp/public/707/cisco−sa−20070124−crafted−tcp.shtml

* Aviso de Seguridad de Cisco: Vulnerabilidad de alteración de la opción IP − http://www.cisco.com/warp/public/707/cisco−sa−20070124−crafted−ip−option.shtml

* Aviso de Seguridad de Cisco: Vulnerabilidad en encabezado de ruteo de IPv6 − http://www.cisco.com/warp/public/707/cisco−sa−20070124−IOS−IPv6.shtml

---

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

- J. Inés Gervacio Gervacio (jgervacio at seguridad dot unam dot mx)
- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- David Jiménez Domínguez (djimenez at correo dot seguridad dot unam dot mx)

UNAM−CERT
Equipo de Respuesta a Incidentes UNAM
Departamento de Seguridad en Cómputo
E−Mail: seguridad@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