UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2008−010

Actualización de Cisco para múltiples vulnerabilidades

Cisco ha publicado una el Boletín de Seguridad cisco−sa−20080326−bundle para corregir múltiples vulnerabilidades que afectan a Cisco IOS. Los intrusos podrían explotar estas vulnerabilidades para obtener acceso a información sensible o para causar una negación de servicio.

Fecha de Liberación: 27 de Marzo de 2008

Ultima Revisión: 27 de Marzo de 2008

Fuente: CERT/CC

Riesgo

Moderado

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas Afectados

- Cisco IOS

II. Descripción

La Alerta de Seguridad cisco−sa−20080326−bundle describe las vulnerabilidades que afectan al IOS de Cisco en su versiones 12,0, 12,1, 12,2, 12,3, y 12,4. Para más detalles se pueden consultar las notas de vulnerabilidades del US−CERT.

III. Impacto

El impacto de esta vulnerabilidad es variable. Las consecuencias potenciales más importantes incluyen la exposición de información sensible y negación de servicio.

IV. Solución

Aplicar la actualización

Los detalles de ésta vulnerabilidad se describen en el Boletín de Seguridad cisco−sa−20080326−bundle.

V. Referencas

- Notas de vulnerabilidades del US−CERT − <http://www.kb.cert.org/vuls/byid?searchview&query=cisco−sa−20080326−bundle>
- Cisco Security Advisory cisco−sa−20080326−bundle − <http://www.cisco.com/warp/public/707/cisco−sa−20080326−bundle.shtml>
- Cisco Security Advisory: Cisco IOS Virtual Private Dial−up Network Denial of Service Vulnerability − <http://www.cisco.com/warp/public/707/cisco−sa−20080326−pptp.shtml>
- Cisco Security Advisory: Multiple DLSw Denial of Service Vulnerabilities in Cisco IOS − <http://www.cisco.com/warp/public/707/cisco−sa−20080326−dlsw.shtml>
- Cisco Security Advisory: Cisco IOS User Datagram Protocol Delivery Issue For IPv4/IPv6 Dual−stack Routers − <http://www.cisco.com/warp/public/707/cisco−sa−20080326−IPv4IPv6.shtml>
- Cisco Security Advisory: Vulnerability in Cisco IOS with OSPF, MPLS VPN, and Supervisor 32, Supervisor 720, or Route Switch Processor 720 − < http://www.cisco.com/warp/public/707/cisco−sa−20080326−queue.shtml>
- Cisco Security Advisory: Cisco IOS Multicast Virtual Private Network (MVPN) Data Leak − <http://www.cisco.com/warp/public/707/cisco−sa−20080326−mvpn.shtml>

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

- Ruben Aquino Luna (raquino at seguridad dot unam dot mx)
- Israel Becerril Sierra (ibecerril 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