UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2006−012

Vulnerabilidad de Race Condition en Sendmail

El CERT/UNAM−CERT, a través de sus equipos de respuesta a incidentes de Seguridad en Cómputo, informan que existe una vulnerabilidad de race condition en Sendmail podría permitir a un intruso ejecutar código arbitrario.

Fecha de Liberación:	22 de Marzo de 2006
Ultima Revisión:	22 de Marzo de 2006
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión

Sistemas Afectados

Sendmail <=8.13.5

Riesgo

Alto

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Race Condition

I. **Descripción**

Sendmail contiene una vulnerabilidad del tipo race condition, causada por el inadecuado manejo de señales de sincronización. En particular, forzando el servidor SMTP para tener un timeout de entrada/salida en el instante adecuado, un atacante podría ejecutar código arbitrario con los privilegios del proceso de Sendmail.

Se pueden consultar más detalles, incluyendo los sistemas afectados en la siguiente nota de vulnerabilidad:

VU#834865 − Vulnerabilidad del tipo race condition en Sendmail
Una vulnerabilidad del tipo race condition en Sendmail podría permitir a un intruso ejecutar código arbitrario. (CVE−2006−0058)

Favor de referirse a la nota de vulnerabilidad de Sendmail y a la página de la versión de Sendmail 8.13.6 para obtener mayor información.

II. Impacto

Un atacante remoto no autenticado podría ejecutar código arbitrario con los privilegios del proceso Sendmail. Si Sendmail se ejecuta como root, el atacante podría tomar control completo de un sistema afectado.

III. Solución

Actualizar Sendmail

La versión 8.13.6 de Sendmail ha sido liberada con el fin de corregir la vulnerabilidad, además Sendmail 8.13.6 corrige otros avisos de seguridad y debilidades potenciales en el código.

Las actualizaciones para corregir esta vulnerabilidad en versiones de Sendmail 8.12.11 y 8.13.5 también están disponibles.

IV. Apéndice A. Referencias

- US−CERT Vulnerability Note VU#834865 − http://www.kb.cert.org/vuls/id/834865
- Sendmail version 8.13.6 − http://www.sendmail.org/8.13.6.html
- Sendmail MTA Security Vulnerability Advisory − http://www.sendmail.com/company/advisory
- Sendmail version 8.12.11 Patch − ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0
- Sendmail version 8.13.5 Patch − ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0
- CVE−2006−0058 − http://cve.mitre.org/cgi−bin/cvename.cgi?name=CVE−2006−0058

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)
- Sergio Alavez Miguel (salavez at seguridad dot unam dot mx)
- J. Inés Gervacio Gervacio (jgervacio at 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