UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2007−022

ServerProtect de Trend Micro contiene múltiples vulnerabilidades

---

Existen un número de vulnerabilidades en el producto antivirus ServerProtect de Trend Micro. Estas vulnerabilidades podríanpermitir a un intruso remoto comprometer de forma total un sistema afectado.

Fecha de Liberación:	23 de Agosto de 2007
Ultima Revisión:	24 de Agosto de 2007
Fuente:	CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como foros y listas de discusión.

Riesgo

Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Múltiples vulnerabilidades

I. Sistemas afectados

- ServerProtect Trend Micro para Windows/Novell Netware

II. Descripción

Múltiples vulnerabilidades de buffer overflow y una vulnerabilidad de overflow de entero han sido descubiertas en las interfaces RPC utilizadas por varios componentes en el paquete de software

ServerProtect de Trend Micro. Estas vulnerabilidades podrían ser explotadas por un atacante remoto con la habilidad para suministrar un requerimiento RPC creado de forma maliciosa al sistema ejecutando el software afectado.

Para mayor información sobre las vulnerabilidades puede consultar la Base de Datos de Notas de Vulnerabilidad.

III. Impacto

Un atacante remoto no autenticado podría ejecutar código arbitrario en un sistema vulnerable. El código suministrado por el atacante podría ser ejecutado con los privilegios de sistema, dando como resultado un compromiso total del sistema afectado.

IV. Solución

Aplicar actualizaciones de Trend Micro

Trend Micro ha proporcionado una actualización para estas vulnerabilidades en:

ServerProtect 5.58 for Windows NT/2000/2003 Security Patch 4 − Build 1185

Se recomienda a los administradores revisar esta nota y aplicar la actualización tan pronto como sea posible.

Restringir el acceso desde la red para los componentes afectados

Hasta que una actualización pueda ser aplicada se puede bloquear el acceso al software vulnerable desde fuera del perímetro de la red, bloqueando específicamente el acceso a los puertos utilizados por el servicio ServerProtect (5186/tcp) y el servicio ServerProtect Agent (3628/tcp). Esto limitará la exposición a ataques; sin embargo, los atacantes dentro del perímetro de la red podrían aún explotar las vulnerabilidades.

V. Referencias

- Notas de Vulnerabidad del US−CERT para Trend Micro ServerProtect Security Patch 4 − <http://www.kb.cert.org/vuls/byid?searchview&query=spnt_558_win_en_securitypatch4>
- README for Trend Micro ServerProtect 5.58 for Windows NT/2000/2003 Security Patch 4 − Build 1185 − <http://www.trendmicro.com/ftp/documentation/readme/spnt_558_win_en_securitypatch4_readme.txt

---

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

- Jesús Ramón Jiménez Rojas (jrojas at seguridad dot unam dot mx)
- Roberto Sanchez Soledad (rsanchez 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