UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−009

El software Backup Exec de Veritas está siendo explotado activamente

---

Backup Exec Remote Agent para Windows de VERITAS contiene un buffer overflow que podría permitir a un intruso remoto, no autenticado comprometer un sistema y ejecutar código arbitrario con privilegios administrativos

Fecha de Liberación: 29 de Junio de 2005

Fuente: CERT/CC y diversos reportes de Equipos de Respuesta a Incidentes, así como Foros y Listas de Discusión.

I. Sistemas Afectados

- **VERITAS Backup Exec** Remote Agent

II. Descripción

VERITAS Backup Exec es una solución de respaldo y recuperación de datos con el soporte para respaldos basados en red. El agente remoto VERITAS Backup Exec está instalado en sistemas que tienen que ser respaldados. Éste escucha en el puerto 10000/TCP para mensajes que indican que un respaldo debe ser realizado.

El agente remoto falla al validar apropiadamente los paquetes entrantes, los cuales permiten que ocurra un buffer overflow. Los mensajes de autenticación especialmente creados pueden ser utilizados para activar el buffer overflow, haciendo posible para un intruso no autenticado explotar esta vulnerabilidad.

El código del exploit para esta vulnerabilidad está disponible ampliamente. Además, se han recibido reportes acerca de que esta vulnerabiidad está siendo ampliamente explotada para ejecutar código arbitrario con privilegios del sistema local. Se ha identificado el incremento de escaneos en el puerto 10000/TCP. Esto incrementa los intentos por localizar sistemas ejecutando el agente remoto VERITAS Backup Exec.

US−CERT está dando seguimiento a este problema en la siguiente nota de vulnerabilidad:

- VU#492105 − El agente remoto VERITAS Backup Exec falla al validar las peticiones apropiadamente. VERITAS identifica este problema en la nota de seguridad VX05−002 y CAN−2005−0773.

Además, US−CERT está investigando otra vulnerabilidad en el software de respaldo VERITAS:

- VU#352625 − El servicio VERITAS Backup Exec Server contiene una vulnerabilidad buffer overflow. VERITAS identifica este problema en la nota de seguridad VX05−006.
- VU#584505 − Vulnerabilidad de validación de acceso remoto en VERITAS Backup Exec. VERITAS identifica este problema en la nota de seguridad VX05−003.

III. Impacto

Un atacante remoto no autenticado podría ejecutar código arbitrario con privilegios de administrador en el sistema vulnerable.

IV. Soluciones

Aplicar actualizaciones.

VERITAS ha publicado actualizaciones para cada versión vulnerable de Backup Exec Remote Agent. Mas informaciòn a cerca de estas actualizaciones se pueden encontrar en el resumen de actualizaciones de Security Advisories VX05−001, VX05−002,VX05−003, VX05−005, VX05−006, VX05−007.

Restringir acceso.

Se recomienda realizar los siguientes pasos para reducir cambios de explotación.

- Usar un firewall para limitar la conección de tal manera que sólo el servidor de respaldo tenga acceso al sistema para respaldarlo. El puerto estándar para este servicio es 10000/tcp.
- En la medida de lo posible, implementar una protección perimetral de red. Al desarrollar las reglas para el filtrado de tráfico de red, procurar que las instalaciones individuales no operen en puertos estándar.

V. Apéndices

Referencias

- US−CERT Vulnerability Note VU#492105 − http://www.kb.cert.org/vuls/id/492105
- US−CERT Vulnerability Note VU#352625 − http://www.kb.cert.org/vuls/id/352625
- US−CERT Vulnerability Note VU#584505 − http://www.kb.cert.org/vuls/id/584505
- VERITAS Software Security Advisory VX05−002 − http://seer.support.veritas.com/docs/276604.htm
- VERITAS Software Security Advisory VX05−006 − http://seer.support.veritas.com/docs/276607.htm
- VERITAS Software Security Advisory VX05−003 −

http://seer.support.veritas.com/docs/276605.htm
- VERITAS Software Security Announcement − http://seer.support.veritas.com/docs/277428.htm
- iDefense security advisory − http://www.idefense.com/application/poi/display?id=272&type=vulnerabilities

---

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 ()
- Sergio Alavez ()

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