UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Boletin de Seguridad UNAM−CERT−2005−012

VERITAS Backup Exec utiliza credenciales de autenticación hardcoded

---

VERITAS Backup Exec Remote Agent para Windows Servers utilizan credenciales de autenticación administrativas hardcoded. Un intruso con conocimiento de estas credenciales y acceso al Remote Agent podría obtener archivos arbitrarios de un sistema vulnerable.

Fecha de Liberación: 12 de Agosto de 2005

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

Sistemas Afectados

Servidores Windows	**VERITAS Backup Exec Remote Agent**	==Todas las versiones

I. Descripción

VERITAS Backup Exec Remote Agent para Windows Servers es una solución de respaldo y restauración de datos que soporta NP (Network Data Management Protocol). NDMP "... es un protocolo estándar abierto para respaldos empresariales de almacenamientos de red heterogéneos". De forma predeterminada, Remote Agent escucha el tráfico NDMP en el puerto 10000/tcp.

VERITAS Backup Exec Remote Agent utiliza credenciales de autenticación administrativa hardcoded. Un intruso con conocimiento de estas credenciales y acceso a Remote Agent podría ser capaz de obtener archivos arbitrarios desde un sisetma vulnerable. El Remote Agent se ejecuta con privilegios de SYSTEM.

Código de exploit, incluyendo las credenciales, ha sido expuesto públicamente. El US−CERT/UNAM−CERT también han visto reportes de incrementos en actividad de escaneo en el puerto 10000/tcp. Esto incremento podría ser

causado por intentos de localizar sistemas vulnerables.

El US−CERT está dando seguimiento a la vulnerabilidad como VU#378957.

Se debe hacer notar que VERITAS fue adquirido recientemente por Symantec.

II. Impacto

Un intruso remoto con conocimiento de las credenciales y acceso a Remote Agent podría ser capaz de obtener archivos arbitrarios de un sistema vulnerable.

III. Solución

- **Restringir el acceso**

  El US−CERT recomienda tomar las siguientes acciones para reducir las oportunidades de explotación.

  - ◊ Utilice un firewall para limitar la conectividad para que solo servidores de respaldo autorizados pueden conectarse al Remote Agent. El puerto predeterminado para este servicio es el 10000/tcp.
  - ◊ Como mínimo, se debe implementar alguna protección básica en el perímetro de la red. Cuando se desarrollan reglas para filtrar el tráfico de red, se debe analizar que instalaciones individuales podrían operar en puertos no estándar.
  - ◊ Además, cambiando el puerto predeterminado del Remote Agent de 10000/tcp podría reducir las oportunidades de explotación. Consulte el documento de soporte 255174 de VERITAS para instrucciones de como cambiar el puerto predeterminado.

Para mayor información, consulte la Nota de Vulnerabilidad del US−CERT VU#378957.

IV. Apéndice A. Referencias

- Nota de Vulnerabilidad del US−CERT − <http://www.kb.cert.org/vuls/id/378957>
- Vulnerabilidad de Descarga de Archivo Arbitrario en Veritas Backup Exec Remote Agent para Windows Servers − <http://securityresponse.symantec.com/avcenter/security/Content/14551.html>
- Documento de soporte de VERITAS 255831 − <http://seer.support.veritas.com/docs/255831.htm>
- Documento de soporte de VERITAS 258334 − <http://seer.support.veritas.com/docs/258334.htm>
- Documento de soporte de VERITAS 255174 − <http://seer.support.veritas.com/docs/255174.htm>
- ¿Qué es NDMP? − <http://www.ndmp.org/info/faq.shtml#1>

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)
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