UNAM−CERT

Departamento de Seguridad en Cómputo

DGSCA−UNAM

Vulnerabilidad de Seguridad UNAM−CERT−2005−492

Buffer Overflow en el Preprocesador de Back Orifice de Snort.

Se reportó una vulnerabilidad en Snort, que puede explotarse para comprometer un sistema vulnerable.

Fecha de Liberación:	18 de Octubre de 2005
Ultima Revisión:	19 de Octubre de 2005
Fuente:	Neel Mehta, ISS X−Force 207

Sistemas Afectados

Snort	<=2−4.2

Riesgo

Altamente Crítico

Problema de Vulnerabilidad

Remoto

Tipo de Vulnerabilidad

Buffer Overflow

I. **Descripción**

Neel Metha reportó una vulnerabilidad en Snort, que puede explotarse por personas malicosas para comprometer un sistema vulnerable.

- La vulnerabilidad es ocasionada rab un errab en el control de los límites de la memoria al manejar los paquetes de Back Orifice. Esto puede explotarse para enviar paquetes UDP maliciosos a una red o dispositivo protejido pab un sistema IDS o IPS con Snort.

  Una explotación exitosa permitira la ejecución de código arbitrario.