Prevent hackers, worms & viruses from using buffer overflows to introduce malicious code into your systems!

SYS-MANAGE

BUFFERSHIELD 1.01

BufferShield is security software, capable of detecting and preventing attempts to execute code on the stack and the heap memory area, in order to stop the exploitation of buffer overflows.

Upon detection it creates an entry within the event log and optionally terminates the application in question, preventing the execution of potentially malicious code.

Buffer overflows are commonly used by hackers to introduce malicious code into your systems.

For example the LovSan/MSBlaster virus used such a buffer overflow to attack remote systems.

Technically **BufferShield** enhances the operating system's memory manager to provide software based support for non executable pages, used to protect the heap and stack memory area.

The product is a very useful addition to Windows Update, minimizing the risk of unresolved security issues, caused by buffer overflows.

Features:

- Detects code execution on the stack, default heap and dynamic heap

- Can terminate applications in question if a buffer overflow was detected

- Reports to the Windows-2000 event log in case of any detected overflows

- Allows the definition of a protection scope to either protect only defined applications or to exclude certain applications or memory ranges from being protected

- **BufferShield** is an affordable alternative for developers, testing their applications for Windows-XP SP2 readiness, without requiring a 64-Bit computer system**.**

Microsoft offers a similar, but hardware based protection, supporting 64-Bit processors like the AMD K8 or the Intel Itanium, starting with Windows-XP Service Pack 2.

Platform:

Windows 2000 / XP / 2003

SYS-MANAGE
http://www.Sys-Manage.com

Sys-Manage A.Denter e.K.
Zehnmorgenstr. 48 - 50, 60433 Frankfurt / Germany
Voice: +49 69 97981082 Fax +49 69 97981083
Internet: http://www.Sys-Manage.com