



**PITBULL®**

# PitBull Foundation and Buffer Overflows

## Buffer Overflow Attacks

Buffer overflow attacks (BOA) are a form of computer breach where a malicious user takes advantage of coding flaws to insert new instructions into a running program. In a BOA, the attacker interacts with a running program and inputs a larger amount of data into a storage area (buffer) of the computer program than it was designed to store. If the programmer did not code the program to check for this kind of user error, the “data” can spill over the memory reserved for the data and overwrite the machine instructions that make up the program itself. The BOA will input executable code instead of whatever data the program was expecting, and when the computer runs that part of the program that has been modified with the attacker's code, it will perform whatever instructions the attacker had inserted. The attacker can thus get access to any data being processed by the program, and if the program was running with special capabilities (such as superuser or administrator privilege), the attacker will be able to access and modify parts of the computer system unrelated to the original program.



**PITBULL®**

## PitBull Foundation

PitBull Foundation is an operating system enhancement that significantly elevates the ability of the system to control what a program can access and how it can use extra security capabilities such as superuser or administrator powers. PitBull Foundation replaces the standard superuser capability with over 100 *privileges*, where each privilege grants only a small fraction of the power of the original superuser power. Programs that normally must run as superuser in order to perform a few special operations can instead be run with the appropriate privilege that severely limits the program from doing anything other than what it was designed to do. In addition to enhancing the privilege mechanism of the operating system, PitBull Foundation also creates operating-system-enforced *compartments* that prevent a program from accessing file system or networking resources that it was not designed to access.

## PitBull Foundation Protection in Buffer Overflow Attacks

PitBull Foundation does not prevent buffer overflow attacks. It does, however, effectively control the damage that can be caused by a program that has been hijacked using a buffer overflow attack. Because programs on a PitBull Foundation system run at a greatly reduced privilege level, hijacked programs almost never are able to give the attacker any significant access to additional system capabilities. Combined with the privilege mechanism, the compartmentalization offered by PitBull Foundation effectively isolates all programs so that no matter how severe the buffer overflow problem, the hijacked program can never affect other programs, attack system resources, or misuse networks connected to the computer. Although PitBull Foundation does not prevent an attacker from accessing or modifying internal program data, it effectively protects all other parts of the system and network from being compromised or damaged by the buffer overflow attack.



### Argus Systems Group

1809 Woodfield Drive

Savoy, IL 61874 USA

Tel: +1 217 355-6308

Email: [info@argus-systems.com](mailto:info@argus-systems.com)

URL: [www.argus-systems.com](http://www.argus-systems.com)