



# Comodo Launches Free Diagnostic Tests to Determine Effectiveness of Desktop Security Solutions

Comodo Inc, September 19, 2007

URL: <http://www.pr9.net/comp/software/6363september.html>

*Tests are designed to determine if Anti-Virus, Firewall and other desktop security software are able to protect against buffer overflow attacks - one of the most prevalent threats on the Internet today.*

PR9.NET September 19, 2007 - JERSEY CITY, N.J., - In its continuing commitment to keep users PCs safe from malware, Comodo today announced an important set of free diagnostic tests that will help users understand how vulnerable their computers are to buffer overflow attacks. Buffer overflow attacks can take many forms, including stack attacks, heap attacks and ret2libc attacks. In each case, the goal is to destabilize or crash a computer system by deliberately causing a buffer overflow - creating the opportunity for the hacker to then run malicious code and even gain control of the entire operating system.

Buffer overflow attacks are emerging as one of the Internet's most sinister mechanisms for injecting malware onto a user's computer. New "drive by download" attacks occur when a visitor navigates to a site that injects malware onto the PC, often by exploiting the vulnerability operative in the memory buffer. In fact, according to Secunia.com - a security information resource, 3 of the top 10 most searched threats are related to buffer overflow attacks [http://secunia.com/advisory\\_statistics/](http://secunia.com/advisory_statistics/).

From a technical perspective, there are three variants of buffer overflow attacks that are very prevalent on the Internet today:

\* Stack overflow:

A stack overflow attack occurs when too much memory is used on the call stack, the limited amount of memory used to run many program functions.

\* Heap Overflow:

Heap overflow is another type of buffer overflow attack that occurs when the dynamic memory allocation needed by the application is flooded causing a crash.

\* Ret2libc Attacks:

A return-to-libc attack is an attack usually starting with a buffer overflow, in which the return address on the stack is replaced by the address of another function in the program and the correct portion of the stack is overwritten. This attack is one of the most difficult to detect and, hence to defend against.

Comodo created its free diagnostic tests to help users understand how well prepared they are to defend against these types of attacks. Each test is a small non-destructive program that deliberately attempts to by-pass the current measures of existing security software. Based on the results of these tests, users can then take remedial action including downloading Comodo's free solutions such as its award winning Comodo Firewall Pro and Comodo Memory Guardian, a new solution (now in BETA) effective at stopping 90%+ of buffer overflow attacks in both 32 bit and 64 bit environments.

"Users should be able to test if their security products such as anti-virus and firewall can protect them from a buffer overflow attack," said Melih Abdulhayoglu, CEO and Chief Security Architect of Comodo. "These attacks are now very widespread and are especially harmful for users because drive-by-download attacks extensively utilize the buffer overflow to inject malware to user's machines. With our combination of free solutions, user can stay safe despite these prevalent threats."

To download these tests, please click here [http://forums.comodo.com/comodo\\_memory\\_guardian\\_buffer\\_overflow\\_protection-b97.0/](http://forums.comodo.com/comodo_memory_guardian_buffer_overflow_protection-b97.0/) (please note that free registration to the Comodo Forum is required to get these downloads if one is not currently a member). To download our free firewall, please visit <http://www.personalfirewall.comodo.com>. To download the BETA version of Comodo Memory Guardian, please click here [http://forums.comodo.com/comodo\\_memory\\_guardian\\_beta\\_corner-b98.0/](http://forums.comodo.com/comodo_memory_guardian_beta_corner-b98.0/)

###

## About Comodo Inc

Comodo, through its group of Internet security companies, is a leading Certification Authority and global provider of Identity and Trust Assurance services on the Internet. Comodo secures and authenticates online transactions and communications for over 1,000,000 business and millions of consumers. With a global presence in the US, UK, Ukraine, and India, Comodo offers businesses and consumers third-generation solutions for intelligent security and authentication technologies that create trust online. Comodo's technological expertise includes PKI digital certification, integrated authentication infrastructure services, regulatory compliance solutions and digital e-commerce services. The Comodo companies develop technologies that address critical authentication and security needs with proven and reliable solutions such as SSL certificates, Mutual Authentication solutions, PCI compliancy services, Desktop Security, Code signing certificates, identity and vulnerability management solutions.

**Phone:** 1 888 266 6361  
**FAX:** 1 201 963 9003  
**Website:** <http://www.comodogroup.com>  
**E-Mail:** [media-relations@comodo.com](mailto:media-relations@comodo.com)

**Address:** 525, Washington Blvd,  
Jersey City  
NJ 07310  
USA

---

[PR9.NET - Your Free Press Release Service](#)