

20 June 2009

By: Lucian Constantin, Web News Editor



New easy to use
HTTP denial of service
method puts web
servers at risk
L'Atelier North America

[Web Servers in Danger from Low Bandwidth HTTP DoS](#)

New attack capable of rendering web servers unresponsive with ease

A new type of attack launched from a single machine with limited hardware resources and bandwidth can cripple many of the webservers on the Internet today. Instead of flooding the server with more packets than it can handle, this new denial of service condition implies sending only a couple of hundreds of partial HTTP requests.

This new DoS attack method has recently been [documented](#) by reputed web security researcher Robert "RSnake" Hansen. The researcher also released a proof-of-concept tool that is able to carry out such attacks. Dubbed Slowloris and coded in Perl, the script can be run from *NIX-based systems only, because Windows limits the number of opened sockets.

This attack is actually the opposite of the classic DoS, as the idea behind it is not to send a huge number of data packets, but rather to trick the destination into waiting for them. In the case of webservers, this is achieved via incomplete HTTP requests.

The attacker opens a full TCP connection to the server and sends it the beginning of an HTTP request. This will force the server to keep the socket opened while expecting for the request to finish. In order to avoid timeouts, more request headers can be subsequently sent at certain intervals, without actually completing it.

Eventually, the webserver's limit of open sockets will be reached and it will become unresponsive to anyone else trying to access it. The attack is rather incremental, because it has to wait for other sockets to be freed before it can consume them, but in the end, it is very efficient and stealthy.

Such an attack targets particular web server instances. For example, if multiple web servers run on a single computer, only the targeted instance will be affected, leaving admins scratching their head as to the cause of the unresponsiveness. Additionally, no errors will be logged until the HTTP requests are completed or canceled.

Web servers like Apache 1.x, Apache 2.x, dhttpd, GoAhead WebServer or Squid have been found to be vulnerable. However, IIS6.0, IIS7.0, lighttpd are not affected. "This is obviously not a complete list, and there may be a number of variations on these web-servers that are or are not vulnerable," the research points out.

Robert Hansen devised the technique based on the previous [research](#) of Robert E. Lee and the [late](#) Jack C. Louis, who discovered severe vulnerabilities buried deep inside almost all TCP-stack implementations that can be exploited in a similar way.

However, Adrian Ilarion Ciobanu, a Romanian system administrator [presented](#) a very similar HTTP DoS concept on the SecurityFocus mailing list back in 2007. "So although there was no tool released at that time he still technically deserves all the credit for this. I apologize for having missed this post," writes RSnake on his blog.