

9 August 2008

By: Lucian Constantin, Web News Editor

[Patch for the Internet Core Flaw Is also Flawed](#)

Proof-of-concept exploit for the patch was released



DNS Patch is flawed
Agder University
College

Yesterday, Russian physicist Evgeniy Polyakov [posted](#) on his blog a [proof-of-concept exploit](#) that is able to insert poisoned DNS entries into a patched server. His setup consisted of two desktop computers and a GigE connection. The successful exploit took place in a bit under 10 hours, which could mean that less time would be necessary with a more powerful setup. Earlier this year, Dan Kaminsky, a security researcher, discovered a security flaw in DNS (Domain Name System) that posed a huge risk to the entire Internet. The industry rushed to come up with a solution and, in early July, they [released a patch](#). Kaminsky released his findings only to a number of big companies, refusing to offer technical details about this vulnerability to the general public until August at a conference in Vegas, when he also [revealed](#) that this flaw might not only affect the web, but also other services like e-mail. Since first announced, this vulnerability has generated a lot of [controversy](#). Security analysts noted that attacks have already been carried out and more will follow. These attacks focused on distribution of malicious software and phishing for personal information, which put financial organizations at risk. Estimates say that the patch for this vulnerability has been installed on 3/4 of the servers worldwide, but Mr. Polyakov's example goes to show that this doesn't make much of a difference. To be more exact, without the patch, an attack could be carried out in seconds, while with the patch it becomes a matter of hours. Paul Mockapetris, the developer of the original DNS, commented that the implementation of this patch is like "playing Russian roulette with a gun that has 100 bullet chambers instead of six." Experts are trying to come up with other, more stable solutions. One of these proposed solutions is DNSSEC, which offers encryption-based addressing and that has already been implemented by some governments, like the Swedish one. However, DNSSEC poses implementation problems for commercial internet because it requires a more solid server infrastructure and a lot more resources compared with normal DNS. This makes DNSSEC a real solution only in the long run, as it can't be introduced and adopted overnight. Others think there are better alternatives to DNSSEC, like Daniel J. Bernstein, a mathematician who developed a DNS version that is not affected by this flaw. His opinion about DNSSEC is that it "offers a surprisingly low level of security, while at the same time introducing performance and reliability problems."