# Researchers Prematurely Expose DNS Security Flaw

By Stefanie Hoffman, ChannelWeb
2:50 PM EDT Tue. Jul. 22, 2008

Researchers at two security companies prematurely leaked details on Monday of a critical Domain Name System (DNS) flaw, which could lead potential attackers to unleash cache poisoning attacks on users' computers.

Details of the DNS flaw were revealed on two separate blog posts before they were set to be publicly disclosed by security researcher Dan Kaminsky at the Black Hat USA 2008 conference during the first week of August.

The DNS error, affecting numerous platforms and vendors, stems from a fundamental flaw in the DNS protocol, a function which provides a back and forth translation of host URLs to IP addresses.

The vulnerability could be exploited by attackers to launch cache poisoning attacks by creating fake messages accepted by the DNS that can trick the server into delivering an incorrect request. Attackers could then use the flaw to redirect Internet traffic to malicious Web sites and install arbitrary code on users PCs.

Details of the DNS bug were recently exposed to the public when Zynamics.com CEO Thomas Dullien, who goes by the blog pseudonym Halvar Flake, speculated on the details in an extensive blog post.

Following Dullien's posting, researchers at Matasano Security then confirmed Dullien's hypothesis, which was subsequently taken down minutes after being posted on the company's site.

The security flaw was first discovered months ago by Kaminsky, director of penetration testing for IOActive, who had been working with vendors like Microsoft (NSDQ:MSFT) and Cisco (NSDQ:CSCO) to create a patch that resolved the DNS error.

Prior to Monday's disclosure, Kaminsky had asked members of the research community to withhold details of the flaw in order to provide users adequate time to patch their systems. He announced that he planned to reveal details of the vulnerability on Aug. 6 during this year's Black Hat USA conference in Las Vegas.

Matasano Principal Thomas Ptacek later apologized to Kaminsky on the company's blog site for prematurely publishing the flaw.

"It was posted in error. We regret that we ran it. We removed it from the blog as soon as we saw it. Unfortunately, it takes only seconds for Internet publications to spread," wrote Ptacek. "We dropped the ball here."

Kaminsky's request that the flaw be kept quiet temporarily sparked controversy for some members of the security research community, who maintained that details of the vulnerability should be open to the public as soon as possible.

In his blog post, Dullien argued that keeping details of the flaw under wraps would ultimately do a disservice to the public.

"I am fully in agreement with the entire way (Kaminsky) handled the vulnerability (e.g. getting the vendors on board, getting the patches made and released, and I understand his decision not to disclose extra information) except the proposed 'discussion blackout,'" wrote Dullien. "In a strange way, if nobody speculates publicly, we are pulling wool over the eyes of the general public, and ourselves."

Because details of the flaw have recently been made public, Kaminsky and other security experts recommend that users patch vulnerable systems as soon as possible.

**"Patch. Today. Now. Yes, stay late," wrote Kaminsky in a blog post on Monday. "Yes, forward to OpenDNS if you have to.** They're ready for your traffic Thank you to the many of you who already have."