DNS Security Flaw Leaked Before Patches Applied

Steve Bosak, newsfactor.com

Tue Jul 22, 7:07 PM ET

A major flaw in the Internet infrastructure was leaked to the public Monday before many IT directors had the chance to apply security patches. The flaw was discovered weeks ago by Dan Kaminsky, a security expert at IOActive, who has worked with industry leading software developers investigating Internet vulnerabilities.

The potential breech is in the current implementation of the Domain Name System for Web servers. DNS is essentially a lookup system for Web servers: names of domains, such as newsfactor.com, are translated by DNS servers to static IP addresses, essentially the true location of the site.

Cause and Cure

A flaw in the DNS caching of incoming requests makes it susceptible to malicious misdirection of Web traffic. If a DNS server does not have an IP address for a requested domain, it asks for this information from another DNS server.

If the clueless DNS server's cache is fooled by malicious information, the user requesting the domain of a legitimate site can be redirected to a spoofed IP address. For example, if a DNS server is fooled into directing legitimate traffic from www.yourbanksite.com to a rogue site, every user hitting the legitimate site would be redirected to the rogue site.

A patch for the flaw was released two weeks ago to corporate and institutional users, but it's unclear how many servers have been fixed and tested. The patch was issued without detailed explanation, but with a strong recommendation to apply it to avoid security breaches. The IOActive Web site includes a link for testing the effectiveness of the patch.

Loose Lips

Speculation circulated around the Internet about what, exactly, Kaminsky discovered. The security researcher was due to make his finding public at the Black Hat hacker's convention in Las Vegas on Aug. 2-7. Kaminsky felt that would give DNS server operators plenty of time to fix the glitch.

But meantime, security experts and benevolent hackers took Kaminsky's silence as a challenge to their abilities. Reportedly, Thomas Dullien, Zynamics.com CEO, posted the flaw on his blog Monday. It was confirmed by another security firm, Matasano. Though the post was removed in minutes, copies quickly circulated throughout the Internet.

A statement on the Matasano blog now reads: "Earlier today, a security researcher posted their hypothesis regarding Dan Kaminsky's DNS finding. Shortly afterward, when the story began getting traction, a post appeared on our blog about that hypothesis. It was posted in error. We regret that it ran. We removed it from the blog as soon as we saw it. Unfortunately, it takes only seconds for Internet publications to spread.

"We dropped the ball here.

"Since alerting the Internet earlier in July about the upcoming announcement of his finding, Dan has consistently urged DNS operators to patch their servers. We confirmed the severity of the problem then and, by inadvertently verifying another researcher's results today, reconfirm it today. This is a serious problem, it merits immediate attention, and the extra attention it's receiving today may increase the threat. The Internet needs to patch this problem ASAP."