DNS Security Flaw Secretly Patched by Multiple Vendors

Mark Long, newsfactor.com

Thu Jul 10, 4:49 PM ET

The U.S. Computer Emergency Readiness Team (CERT) has disclosed the discovery of defects in an essential component of everyday Internet operations.

The flaw was found at the heart of the Domain Name System -- the Internet "phone book" for translating Web URLs into the numerical IP addresses that networking computers use to deliver information. According to CERT, hackers could use a technique called DNS cache poisoning to place forged DNS data into the cache of a name server at any Internet domain.

"An attacker with the ability to conduct a successful cache-poisoning attack can cause a name server's clients to contact the incorrect, and possibly malicious, hosts for particular services," CERT said. "Consequently, web traffic, e-mail and other important network data can be redirected to systems under the attacker's control."

A Flaw in the Core

The underlying DNS defects were brought to CERT's attention by Internet security expert Dan Kaminsky, the director of penetration testing at IOActive.

"There's a bug in DNS, the name-to-address mapping system at the core of most Internet services," Kaminsky said. If "DNS goes bad, every Web site goes bad, and every e-mail goes somewhere," but "not where it was supposed to," he added.

Software companies across the industry have been quietly collaborating to simultaneously release patches for virtually all the affected name servers, Kaminsky said. "We got everyone into a room and hammered out a plan," he recalled in a blog. "After an enormous and secret effort, we've got fixes for all major platforms, all out on the same day."

However, the specific nature of the vulnerability is still being kept under wraps to prevent hackers from knowing precisely where to look.

"This is actually a flaw in the core of DNS itself," Kaminsky said in a recent network security podcast. "What this means is that it isn't something that's in" a Microsoft, ISC, Cisco or some other implementation -- it's in all of them," he said. "And the interesting thing to realize is that DNS, unlike many other technologies, chains very, very well with other vulnerabilities."

A Sledgehammer by Design

To prevent hackers from being able to examine the patches as a means for pinpointing the vulnerability, the collaborators decided to fix the problem by making DNS more random. "This is a sledgehammer, by design," Kaminsky explained in his blog. "It cuts off attack surface, without necessarily saying why."

However, Kaminsky noted that the patch code doesn't always install itself. To help network administrators determine if the DNS servers they use are still vulnerable, he has posted a DNS checker on his blog page at doxpara.com.

Still, Kaminsky said there will be networks unable to use a patch to plug the security hole, and who are "going to need to know how all this works." For this reason, he expects to detail the flaw during next month's Black Hat security conference in Las Vegas.

The patches for improving the resilience of the Internet to this type of attack are only workaround solutions, explained ISC President Paul Vixie.

"The only definitive solution for this threat," Vixie said, will come through the use of DNSSEC (Domain Name System Security Extensions) -- a suite of specifications for securing certain DNS information used on IP networks. "We are redoubling our efforts to make DNSSEC a real option in the near term."