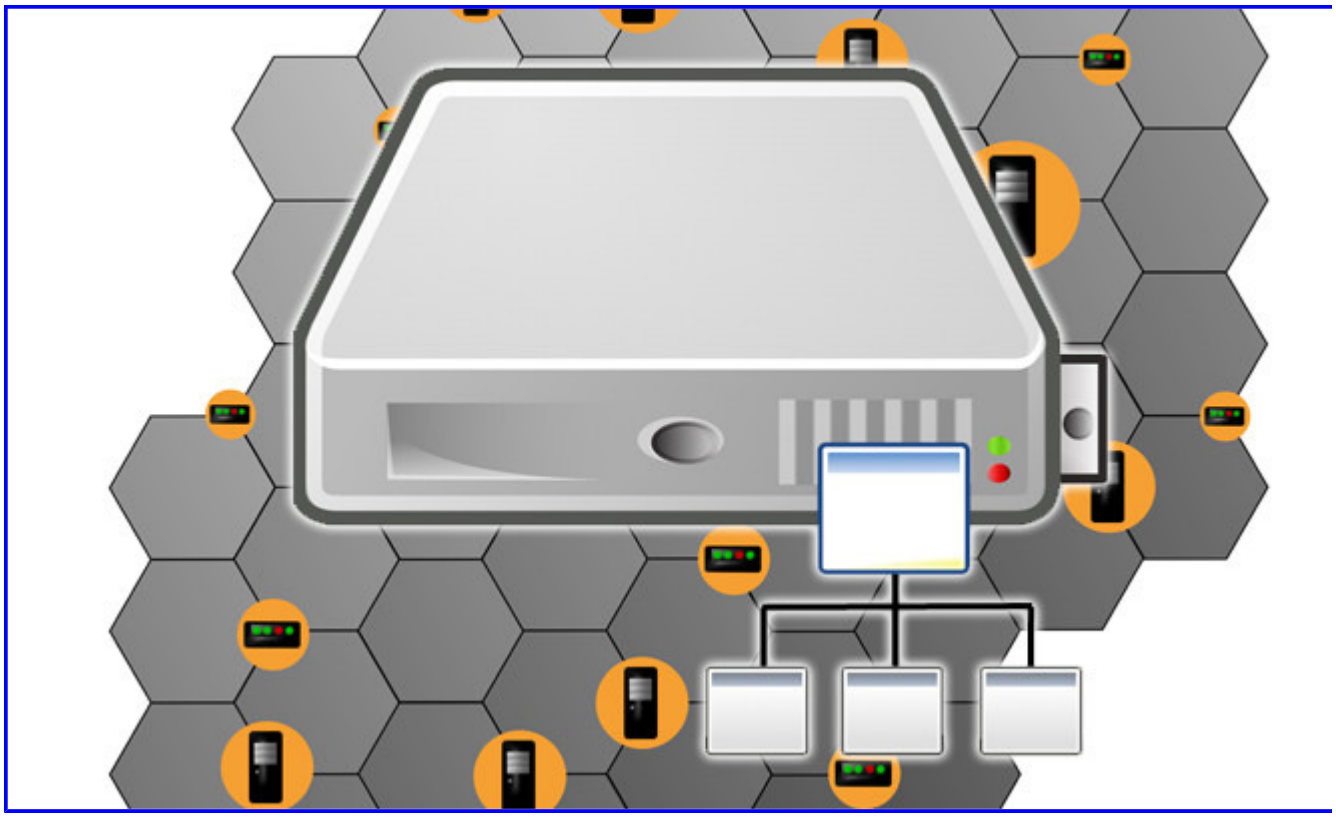

BIND Vulnerability Enables DNS Cache Poisoning Attack

Follow @TheBrianDonohue by Brian Donohue August 13, 2013 , 4:46 pm

A vulnerability in the BIND domain name system (DNS) software could give an attacker the ability to easily and reliably control queried name servers chosen by the most widely deployed DNS software on the Internet, according to new research presented at the Woot Conference in Washington D.C. today.

The Internet Systems Consortium has acknowledged the vulnerability.

Related Posts

Patch Available for DoS Vulnerability in BIND Nameservers

July 29, 2013 , 9:15 am

DDoS Attack Knocks Network Solutions Website, Clients Offline

July 17, 2013 , 3:13 pm

ISC Patches Known BIND 9 DoS Vulnerability

June 6, 2013 , 11:26 am

Researchers Roee Hay of IBM, Jonathan Kalechstein of the Tecnion Computer Science Department, and Gabi Nakibly of the National Electronic Warfare Research & Simulation Center uncovered a vulnerability in BIND's smoothed round trip time (SRTT) algorithm.

The primary mitigation technique for DNS spoofing attacks is IP address randomization. The researchers explain the SRTT algorithm helps BIND choose the resolver with the fastest response time for a particular query from a dynamic list of name servers. This process should be a somewhat random and not easily guessable one. A weakness in that algorithm, however, could give an attacker the ability to de-randomize the SRTT name server selection process, effectively giving that attacker the ability to shorten the amount of time needed to perform a blind DNS cache poisoning attack, a perform man-in-the-middle attack, or assist in distributed denial of service attacks.

Cache poisoning attacks – the most common type of DNS attack – are those in which an attacker causes a victim resolver to cache a fake DNS resource record. In this way, the attacker can cause his victims to communicate with a server under his control without their knowledge. In this sort of attack, a hacker could cache a fake resource record that resolves to an IP address that appears to belong to a software update server but which is actually leading the victim to a malicious server.

The researchers say that the attack essentially reduces the time and effort needed to poison BIND's cache, and that DNS resolvers should never keep a global state shared between different domain names.

You can read their full research paper here.

Tweet 0 • Share on Twitter
Like 52 • Share on Facebook
• Google +1 2
Share 10 • Share on LinkedIn

0
Categories: Vulnerabilities

Leave A Comment

Your email address will not be published. Required fields are marked *

Name *

Email *

Comment