PC MAGAZINE PCMAG.COM BLOGS Security Watch PC MAG.COM NETWORK

Wednesday July 23, 2008

Attack Code Published For Big DNS Flaw

Categories:
DNS, Known Vulnerabilities, Software Patches

Tags:

It was just a matter of time after the premature release of details on the attack: attack code for the big DNS vulnerability patched in many products earlier this month has been released.

The exploit code allows for the insertion of malicious records into the cache of targeted DNS servers. It has been posted to Metasploit whose creator, HD Moore, wrote the exploit with a researcher named "|)ruid " from the Computer Academic Underground.

If you're responsible for a DNS server—not just Windows, but all the major ones—and have not applied this patch, you and your users are at great risk. Patch now.

Tuesday July 22, 2008

Details On Big DNS Flaw Prematurely Released

Categories:
DNS, Known Vulnerabilities, Software Patches

Tags:
blogging, DNS, vulnerabilities

One of the many things that researchers agreed on in the major coordinated fix of a flaw in the DNS earlier this month was to withhold details on the vulnerability itself in order to give users enough time to apply updates. Too bad, another researcher spilled the beans.

Halvar Flake, talented in the ways of reverse-engineering and not, it seems, part of any confidentiality agreement, speculated on the details of the attack in his blog. Flake disagrees on the utility of the 29 day blackout period; he argues that people are better off with more information in this case. He says "It feels like we're all trying to rock the train." (To get the rest of the joke preceding that punch line, read his blog.) Flake dismissed his own expertise and assumed his guess must be wrong, but turns out he was right.

Matasano Security released their own blog on Monday announcing that Flake was right and delving further into the details. They quickly realized they shouldn't have done that and pulled the blog entry, but too late: For instance, my own RSS reader had already gotten the entry and I have a copy of it.

Let's hope that Flake is right and that the silence period is not really advantageous, because the details of the attack became generally known 11 days after the patch, not 29. In the meantime, patch as fast as you can.