

Cache Poisoning Vulnerability in Multiple DNS Implementations

July 28, 2008

DESCRIPTION.

Earlier this month, security researcher Dan Kaminsky released a general description of an easily exploitable DNS vulnerability, regarding which he had coordinated with a number of third party vendors to patch this issue. The details of his research were recently disclosed and inadvertently confirmed by credible parties. Not long afterward, the Metasploit project released exploits against this vulnerability.

The DNS vulnerability regards weak randomization of the source ports and transaction. By combining this with the inherent vulnerabilities of the DNS protocol, one could poison the cache of a nameserver or stub resolver.

ATTACK SCENARIO.

The 16-bit transaction ID and the client's source port are used together to identify unique transactions as well as to provide some safeguarding against injected traffic. The attacker could bypass this safeguard using two methods:

- (1) by interacting with the victim host and observing any predictable patterns in the victim's choice of source port. This reduces the guesswork needed to generate effective fraudulent responses to the resolver's subsequent requests. The cache is then poisoned by submitting an arbitrary IP as the resource record for the target domain.

- (2) by racing an authoritative nameserver's response to a query for a nonexistent subdomain within the target domain, and injecting arbitrary IP addresses into the authoritative resource records. This brute force attempt would likely generate an abnormally high amount of DNS traffic.

DETECTION AND MITIGATION.

As discussed in the previous section, single-packet inspections would be ineffective against such attacks. Setting thresholds would detect brute force attempts to poison the cache, but at the expense of generating false positives also. There may not be an effective solution outside of confirming DNS responses with root nameservers via TCP. Some vendors have released patches to better randomize transaction IDs and source port numbers. Microsoft's recent patch release effectively turned off the DNS caching feature to prevent cache poisoning.

REFERENCE ID.

CVE-2008-1447