Nominum
Connecting Networks and People

Nominum Software Security Advisory NOM-20080708
8-July-2008

Nominum is releasing this software security advisory to its customers regarding a newly found vulnerability in DNS. This important DNS security issue requires immediate attention on the part of your technical and operations staff.

Products Affected
Versions of CNS and Vantio released before June 4th, 2008.

Vulnerability Assessment High.
Cache poisoning allows an attacker to selectively control destination web sites for users accessing a compromised DNS. For example, if a cache entry for Google is poisoned, a user typing in www.google.com would not get the Google website but rather a site controlled by the attacker. This is a serious problem because users believe they are going to a legitimate site, and thus have no reason to suspect they are under attack. Under such circumstances a user may be perfectly comfortable taking a survey that requests confidential information, again since they believe they are at a site they are familiar with and visit often.

Technical Details
Recently, a prominent DNS researcher uncovered a new method of using DNS Query-ID spoofing to poison the DNS cache. This vulnerability is a DNS architectural issue that affects all DNS vendors, and all of the major DNS vendors are collaborating for a coordinated response.

DNS Query ID spoofing has been known for several years. In the past, the techniques for guessing a random 16 bit Query ID and successfully poisoning a cache entry took on the order of a week. Recent research has uncovered a way to reduce this time significantly. Protecting against this vulnerability implies making it harder for the attacker to guess the right data to spoof answers from an Authoritative server.

The vulnerability is described in CERT (United States Computer Emergency Readiness Team) Vulnerability Note VU#800113.

Product Notes
This vulnerability affects all customers using versions of CNS and Vantio released before June 4th, 2008 regardless of what features are being used.

ANS, Navitas IPRD server and SML are not susceptible to this vulnerability, and do not need to be upgraded.

Nominum's Actions
The industry-wide response to this issue is to introduce source UDP port randomization to make it more difficult for an attacker to spoof query requests by adding more bits that need to be guessed.

Nominum made updates to CNS and Vantio to add UDP source port randomization. This feature allows Nominum caching servers torandomly choose an outgoing source UDP port for each outgoing query to provide additional resilience against query ID spoofing attacks. This new capability is supported on a per view basis. The source IP address of the ports is also configurable on a per view basis.

The number of random source ports is configurable with a maximum value of 1024. The optimized number of source ports to use is dependent on the operating system; suggested values are included in the documentation. The starting port number is configurable. The implementation has a varying performance impact depending on the operating system and hardware platform.

Nominum's implementation is compatible with the IETF draft: "Measures for making DNS more resilient against forged answers" which can be found at:

http://www.ietf.org/internet-drafts/draft-ietf-dnsext-forgery-resilience-05.txt

Recommendations for Customers
Nominum made updates to CNS and Vantio available June 4, 2008 and it is strongly recommended these updates be applied immediately.

Further Information
Further information about these issues can be found at the following sites:

http://www.kb.cert.org/vuls/id/800113
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447

Customers in need of additional information or assistance should contact the Nominum Support team at support@nominum.com,
+1.650.381.6091 or +1.877.482.4367 (toll free in the US)