

**Nominum Contact:**

Bruce Van Nice

Nominum

+1.650.381.6308

[bruce.vannice@nominum.com](mailto:bruce.vannice@nominum.com)

## **Nominum's Software Update Protects Networks from New DNS Security Vulnerability**

*Cache poisoning vulnerability requires immediate action to deter Internet exploits*

Redwood City, Calif. – July 9, 2008 — Nominum, the leading provider of network naming and addressing technologies, announced that latest versions of its Caching Name Server and Vantio Base Server software meet and exceed the tightened DNS security measures required to address a new DNS security threat announced by the United States Computer Emergency Readiness Team (US-CERT) Vulnerability notice number 800113 on July 8th, 2008.

Nominum's expertise with DNS and its vantage point in more than 100 carrier networks offers unique insights into security threats. Nominum understands the seriousness of these threats and, prior to the vulnerability, had already developed advanced capabilities that deter them. A software upgrade has already been released that exceeds the measures defined by the IETF and the joint ad hoc group.

The new vulnerability described in the US-CERT advisory is an enhanced cache poisoning attack that allows an attacker to insert false records into unprotected DNS servers, and hijack users to counterfeit sites. From there an attacker can steal passwords or potentially gather other sensitive and valuable information from a completely unsuspecting victim. This kind of phishing attack is especially dangerous because the user believes they are at a familiar site. If Internet users start to believe that they cannot trust the basic infrastructure of the Internet the impact on ecommerce and other Internet transactions is potentially massive.

"The seriousness of this threat mandates immediate action," said Dr. Paul Mockapetris, Nominum's Chief Scientist and inventor of the DNS technology. "Cache poisoning allows an attacker to selectively control destination web sites for users accessing a compromised DNS. Nominum and other selected DNS vendors worked closely with security researchers to define

the unique problems created by this new vulnerability and each vendor developed new software implementations to proactively address potential exploits,” he continued.

The multi-vendor group rapidly implemented UDP Source Port Randomization defined by IETF draft “Measures for making DNS more resilient against forged answers” (draft-ietf-dnnext-forgery-resilience-05.txt) as the solution. Randomizing the UDP port used for DNS queries greatly increases resilience to exploits that take advantage of the new vulnerability. It was implemented quickly and Nominum took steps to proactively get customer networks protected well in advance of the public disclosure.

“Nominum’s focus and commitment is on improving the Internet, and security is a key part of our mission”, said Tom Tovar, CEO of Nominum. “We have a responsibility to every customer and to the 150 million+ users that query our installed base of DNS products every day. Our goal in responding to this vulnerability is to ensure the Internet stays a trusted communication medium for the global online community.”

Nominum’s software implementation uses a more aggressive port randomization approach to fortify CNS and Vantio defenses. Additionally, Nominum invested heavily in advanced capabilities that provide a level of resilience to these security threats that is unmatched in the industry.

Starting with the industry’s only commercial grade DNS caching engine, Nominum has built intelligence into the query path that introduces additional layers of protection from cache poisoning. Support for UDP Source Port Randomization, as part of the effort to deter this latest threat, improves upon the resilience to cache poisoning threats already available in Nominum’s implementations. The advanced design of Nominum’s caching engine ensures high performance even with security features turned on and under attack.

For more information regarding the new software releases and required action, refer to Nominum’s home page: [www.nominum.com](http://www.nominum.com).

### **About Nominum**

Nominum's network naming and addressing solutions power the world's largest always-on networks. Nominum is a global provider of ENUM-based IP-Application Routing Directory, DNS

and DHCP solutions that enable communication providers to deliver high quality always-on broadband internet and innovative services to their customers, including VoIP, push to talk, fixed-mobile convergence, IPTV and triple-play. For further information, visit [www.nominum.com](http://www.nominum.com).