

## DNS Vulnerability Requires More Action Than Patching Alone

Greg Young, Paul E. Proctor, Mark Fabbi

Patches been released for newly announced Domain Name System vulnerabilities that affect products from at least 79 vendors. But enterprises need to take protective measures that extend well beyond normal patching.

## NEWS ANALYSIS

---

### Event

On 8 July 2008, two security vulnerabilities in many Domain Name System (DNS) resolvers discovered by an independent researcher were publicly announced, and vendors of most of the affected software products coordinated the release of multiple server patches for the vulnerability. (Some client-side patches are also available.) The vulnerability, which could potentially allow "spoofing" attacks, is known to affect DNS servers from 79 vendors, as well as other software products that use DNS. Details of the vulnerability and the patches are deliberately being kept vague to make reverse-engineering more difficult, but further information, including a list of affected vendors and products, is available from the United States Computer Emergency Readiness Team (US-CERT) at <http://www.kb.cert.org/vuls/id/800113>.

### Analysis

No exploits for these DNS vulnerabilities had been documented at the time of publication. Microsoft and many of the other affected vendors have given them their second-highest severity ranking, because remote code execution (a requirement for highest severity) is not relevant. Nonetheless, this vulnerability could allow transparent rerouting of traffic or routing of traffic sent to internal addresses outside the enterprise perimeter, potentially exposing sensitive information and increasing the risk of further exploits and external "ownership" of internal networks. Moreover, because exploiting this vulnerability does not result in changes to configuration tables in the application, exploits would be difficult to detect.

The patching process includes a change in DNS interaction designed to make it more difficult to "guess" a transaction ID, which is the reason it spans so many implementations. The patch also changes the usual DNS "handshake" and the DNS query protocol involving port/socket usage via port randomization. Firewalls, routers or DNS proxies may require configuration changes in cases where DNS traffic is expected to use a specific port or socket. If the enterprise firewall limits DNS connections to a single port (typically port 53), this restriction must be removed. At the time of publication, conflicts with personal firewalls that use source port firewalling had been reported.

### RECOMMENDATIONS

---

#### Enterprise security decision-makers:

- Assess whether your DNS servers and DNS resolvers and operating systems are affected, and patch, if necessary, no later than the end of September 2008.
- Scan the network for DNS servers beyond the primary server (for example, in test and development labs or remote geographical locations).
- If any DNS proxies are used, test them to confirm that they can function with the new port behavior required by the patch. If your enterprise tests patches before installation, consider also testing critical components that rely on DNS to function.
- If you are limiting socket ranges for DNS, review the patch notes for your operating systems to determine whether client-side configuration changes are necessary.
- Request a signature update from your intrusion detection system or intrusion prevention system vendor that includes detection of possible exploits using this vulnerability.

- Follow the established best practice of filtering IP addresses at the perimeter to prevent spoofing, such as internal IP addresses coming from external domains.

## RECOMMENDED READING

---

- "Classifying and Prioritizing Software Vulnerabilities" — Enterprises need a structured approach to classifying and ranking software security vulnerabilities. **By John Pescatore**
- "Active Directory and DNS Integration" — DNS and Active Directory integration choices continue to present challenges for IT infrastructure deployments. **By John Enck, Mark Fabbi and Lawrence Orans**

(You may need to sign in or be a Gartner client to access the documents referenced in this First Take.)

## REGIONAL HEADQUARTERS

---

### Corporate Headquarters

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### European Headquarters

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### Asia/Pacific Headquarters

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### Japan Headquarters

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### Latin America Headquarters

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509