

JULY 08 DNS VULNERABILITY



OVERVIEW AND SUGGESTED MITIGATIONS

07/10/08

Overview

Background Information

On July 9th, 2008 a massive effort was made among software and hardware vendors to release a simultaneous patch to their products. This patch was created to mitigate or minimize the effects of a vulnerability discovered in the basic operation of the Internet Domain Name System or DNS. This subsystem is critical to the operation of the Internet and provides for the translation of human readable names into computer usable IP addresses.

Vendors of most major operating systems and network hardware participated in the effort. Each vendor also released their own advisories and patches using their existing patch processes. The US CERT also played a major role in coordinating the release and advises all organizations to test the patches from the vendors and get them applied as soon as possible. While no known malicious activity exists as of the time of this writing, it is largely known that attackers are assembling the details that have been made public and are attempting to recreate the vulnerability and exploitation techniques that the initial researcher discovered.

Disclosure/Discovery and The Exploitation Race

Even as attackers are moving to recreate the vulnerability and exploit, the clock is ticking toward the date of the public disclosure of the vulnerability. The researcher, Dan Kaminsky, plans to release the full details, which will include exploitation techniques, on August 6th, 2008 at the Black Hat Conference in Las Vegas. It is expected at that time that the exploitation of the vulnerabilities will become nearly trivial and will be widespread against unpatched and unprotected systems and environments.

Meanwhile, this window for testing and applying the patch could also close at any time. Attackers are racing to do analysis and to identify the vulnerability and exploitation techniques. There is a large avenue for public fame and obviously, quite a bit of financial and infrastructure damage that could be accomplished using the attack. The quicker the attackers understand and can exploit the vulnerability, the less patched systems there will be and the larger their pool of opportunity.

Basically, this means that organizations have a window that runs from the present until discovery/ disclosure. That could be as long as August 6th, but is very likely to be sooner. All organizations are encouraged to apply the appropriate vendor patches as soon as possible and to implement the additional security measures as described in the section titled "Mitigation".

Further DNS Issues Likely

Keep in mind that even as attackers attempt to reconstruct the initially identified vulnerability and exploit that they are quite likely to find additional security issues in current DNS servers and products. They may identify further protocol or process holes. Certainly, specific instances of DNS products will be found to have additional vulnerabilities that could range from usual buffer overflows to less technical poisoning attacks. As such, it is critical for all vendors to immediately begin security analysis of their DNS products and for all customers to urge their DNS product vendors to complete these reviews and perform mitigations as quickly as possible. Further, security and network management teams MUST immediately begin to analyze their networks and environments cataloging their existing DNS infrastructures and compiling a comprehensive data set of their locations, versions and products used in their organizations. These teams must also remain vigilant and maintain ongoing knowledge of any patches, upgrades or mitigations that their relevant vendors develop in the coming months.

All Internet sites and organizations can expect to see wide scale increases in DNS scanning, probes and exploit attempts, even for already known and published vulnerabilities. History shows that as attackers become focused on specific services, old vulnerabilities typically reemerge as critical and new vulnerabilities are usually identified. As such, organizations should expect that their security teams and network management staff will be facing an onslaught of DNS related activities in the coming months. Budgets, staffing and support mechanisms for this work should be anticipated and planned for by upper management.

Mitigation

First and foremost, organizations are encouraged to identify all instances of DNS servers, stubs resolvers and clients in their environment. Building a catalog of these products is an ESSENTIAL first step to ensuring mitigation for the entirety of an organization. This data can be assembled from network analysis, vulnerability assessment data and other scanning techniques. Pay careful attention during this process to network hardware such as routers, firewalls, DHCP servers and other tools that might be offering firmware-based DNS services but that might not be specifically designed for such uses. These non-traditional DNS implementations are the most likely to be overlooked, forgotten and targeted by attackers even long after the initial interest in these issues has passed.

Next, test and apply all relevant vendor patches. Most operating systems will need to be patched and many network devices will require upgrades/patches to their software and firmware. This is usually a massive effort and may even require physical access to the system to perform the upgrade. As such, staffing and planning must be performed to close this critical hole as soon as possible. The good news is that for many of these devices where firmware upgrades are required, this sudden attention may also result in the mitigation of additional vulnerabilities and issues that have been addressed by the vendor since the last time the device was upgraded/patched, if that has ever occurred.

Once the patches have been applied, any systems remaining in the catalog of DNS services must be addressed. In locations or devices that are unable to be patched or upgraded, the following workarounds should be considered and applied:

- If using BIND 8, the implementation MUST be upgraded to BIND 9 or abandoned/replaced. Mitigation of BIND 8 environments is not thought to be possible at this time and mitigation of the issues in BIND 8 products is not expected.
- Disable recursion wherever possible, but certainly on all Internet-facing systems. If recursion is required, it should be restricted by IP address to only the hosts that are required for proper DNS operation. If you need assistance with this configuration change or in identifying required recursive hosts, contact the product vendor for technical assistance and support. CERT reminds all technical teams that "It is important to understand your network's configuration and service requirements before deciding what changes are appropriate."
- Implement a robust local caching system of your own that is carefully secured and controlled. This will reduce the likelihood of compromise and the effects of compromises of "upstream" implementations. Ensure that any system you put in place is properly shielded and controlled in terms of recursion and Internet exposure.

Organizations are highly encouraged to immediately patch all DNS products that can be patched and to remain vigilant for upcoming product patches and fixes as more information is discovered/disclosed about this and other possible DNS security issues. Patching is the best, strongest and most effective defense possible at this time.

More Information

The following are reliable sources for additional information about this issue as it emerges:

CVE Database: CVE -2008-1447 <http://cve.mitre.org>

CERT: <http://www.kb.cert.org/vuls/id/800113>

SANS Internet Storm Center: <http://isc.sans.org>

State of Security: <http://www.stateofsecurity.com>

Assistance

If your organization would like assistance in understanding this vulnerability or in managing or performing the mitigation process, please feel free to contact MicroSolved, Inc. for assistance. We will be happy to work with your organization to assist you in your efforts to remediate the problems and secure your assets. For more information about this or any of our products and services, please contact an account executive at (614) 351-1237 or via email at info@microsolved.com.

This whitepaper and the contents are copyright MicroSolved, Inc. 2008. All rights reserved.