US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Critical Infrastructure Information Notice- CIIN-08-206-01

July 24, 2008

DNS Cache Poisoning Vulnerability and Mitigation Strategies

Overview

DNS servers employ caches of memory to improve their performance when answering multiple identical queries. When a DNS server answers a query with information that did not originate from an authoritative DNS server, it is considered poisoned. DNS cache poisoning (sometimes referred to as cache pollution) is an attack technique that allows an attacker to introduce forged DNS information into the cache of a caching nameserver. Due to the caching mechanism, a poisoned DNS server will continue to answer queries for the forged information until the cached answer times out.

US-CERT has become aware of deficiencies in DNS implementations that could leave an affected system vulnerable to cache poisoning. US-CERT is issuing this notice to detail these issues and provide mitigation strategies for organizations to implement.

Details

US-CERT first reported on this on July 8th, when multiple vendors released updates to resolve weakness in DNS implementations that could leave vulnerable systems open to cache poisoning. These patches implement source port randomization in the nameserver as a way to reduce the practicality of cache poisoning attacks. US-CERT released Vulnerability Note VU#800113 to detail the vulnerability and provide mitigation strategies.

On July 21st, technical details regarding the vulnerability were posted to public websites. US-CERT issued follow up advisories warning that attackers could use these details to construct exploit code, and urging administrators to patch systems or apply workarounds immediately.

On July 23rd , exploit code for this vulnerability was published claiming to have been tested against BIND versions 9.4.1 - 9.4.2. Exploitation of this vulnerability may allow an attacker to cause a nameserver's clients to contact incorrect and possibly malicious hosts for particular services. As a

result, web traffic, email, and other important network data could be redirected to systems under the attacker's control.

While patches have been released by most vendors, reports have surfaced that in certain cases, the fixes may cause performance degradation issues. Internet Systems Consortium (ISC) states the following in their advisory, "The patches will have a noticeable impact on the performance of BIND caching resolvers with query rates at or above 10,000 queries per second. The beta releases include optimized code that will reduce the impact in performance to non-significant levels." US-CERT is also investigating reports that patched Solaris DNS servers may suffer degradation in performance due to increased overhead required to randomize the source port associated with each query.

In addition to these issues, US-CERT has become aware of a new issue affecting the DNS mitigation strategies and patches provided by vendors that decrease their effectiveness. Administrators should be aware that in infrastructures where nameservers exist behind Network Address Translation (NAT) and Port Address Translation (PAT) devices, port randomization in the nameserver may be negated by the NAT/PAT device and a sequential port address could be allocated. This may weaken the protection offered by source port randomization in the nameserver.

US-CERT has released multiple products including Current Activity entries, a Technical Alert, and Vulnerability Note #800113 (on www.us-cert.gov) to address these DNS issues.

Solution

US-CERT strongly urges organizations to patch affected systems immediately. In addition to this, organizations should consider one of the following workarounds to help mitigate against the NAT/PAT issues as described above:

- Configure the NAT/PAT device to perform source port randomization.
- Configure the NAT/PAT device to preserve the source port assigned by the nameserver.

A NAT/PAT device can eliminate improvements gained by patching DNS software if the device does not preserve the original random source ports, or does not introduce its own source port randomization. If such a device is interfering with the effects of the DNS patch, US-CERT recommends contacting the vendor for information on how to restore source port randomization.

Architectural changes involving the use of additional DNS resources (forwarders) or changing the location of DNS resources (i.e., moving a DNS server outside of a NAT/PAT device) can mitigate the NAT/PAT issue in cases where source port randomization cannot be restored due to the limitations of the NAT/PAT device. However, these architectural changes are complex and unique to each local network environment, and require careful planning and risk-assessment in order to avoid introducing other vulnerabilities into the DNS hierarchy.

Because the ability to spoof IP addresses is necessary to conduct these attacks, administrators should filter spoofed addresses at the network perimeter. IETF Request for Comments (RFC) documents RFC

2827, RFC 3704, and RFC 3013 describe best current practices (BCPs) for implementing this defense.

Any attempt to exploit this vulnerability is expected to be accompanied by a marked increase in inbound traffic from source port 53. Such traffic should be monitored in order to identify possible attacks taking place. DNS logs (when enabled) may also provide data that can be analyzed to detect attacks.

Additionally, a successful attack which poisons the cache for a popular site will likely affect the top destinations visited by a networks' systems. Sudden, unexpected changes in frequently visited site statistics by IP address may indicate that the record has been poisoned and visitors are being sent to an incorrect address.

Organizations should follow their established internal procedures if any suspected malicious activity is observed, and report their findings to US-CERT for correlation against other incidents. US-CERT also reminds organizations that proper impact analysis should be performed prior to taking defensive measures.

The U.S. National Institute of Standards and Technology (NIST) Special Publication 800-81 "Secure Domain Name System (DNS) Deployment Guide" contains detailed and thorough information about the secure deployment of DNS servers, including the recommendations above. Administrators are strongly encouraged to review this document and consider implementing the recommendations it describes.

Additional Resources

US-CERT Vulnerability Note - This vulnerability note will be updated as needed with additional vulnerability and vendor information.

http://www.kb.cert.org/VULS/ID/800113

US-CERT Current Activity

http://www.us-cert.gov/current/index.html#nat_pat_affects_dns_cache

http://www.us-cert.gov/current/#dns_cache_poisoning_public_exploit

http://www.us-cert.gov/current/#dns_implementations_vulnerable_to_cache

Microsoft Security Bulletin MS08-037 (updates)

http://www.microsoft.com/technet/security/Bulletin/MS08-037.mspx

ISC BIND Updates

http://www.isc.org/index.pl?/sw/bind/index.php

McAfee Avert Labs – Diagram of the attack

http://www.avertlabs.com/research/blog/index.php/2008/07/23/the-cat-is-out-of-the-bag-dns-bug/

SANS Internet Storm Center

http://isc.sans.org/diary.html?storyid=4765

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov
Voice: 1-888-282-0870
Incident Reporting Form: https://forms.us-cert.gov/report/

Document FAQ

What is a CIIN? A Critical Infrastructure Information Notice (CIIN) is intended to provide warning to US critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks.

C*an I distribute this document to other people?* This document may be shared with personnel who have a direct role in securing US critical infrastructure networks. If necessary, please contact US-CERT for clarification or specific distribution inquiries.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.