Release software to check DNS server vulnerabilities

According to Bach Khoa Network Security Center (Bkis), DNS cache poisoning vulnerabilities are placing DNS server systems in Vietnam as well as worldwide.

According to Bach Khoa Network Security Center (Bkis), DNS cache poisoning vulnerabilities are placing DNS server systems in Vietnam as well as around the world at the risk of hackers attacking and poisoning on a large scale.

This is a particularly serious vulnerability when hackers have a new way to successfully exploit this vulnerability. This confuses many network administrators when there is no tool to check if their DNS server system has this error and how to fix it.

On July 25, 2008, Bkis released Bkav DNS Check software to allow checking and detecting DNS server system with Subdomain Exploit DNS Cache Poisoning vulnerability. Along with the release of this software, Bkis also instructed how to fix the vulnerability to avoid the risk of outbreaks of DNS attacks in Vietnam.

To check if your system is at fault, network administrators of agencies and ISPs follow these steps:

1. Download Bkav DNS Check at the following address : http://www.bkav.com.vn/DNSCheck/BkavDNSCheck.exe

2. Configure DNS Server Forwarders : to point domain name **BkavDnsCheck.vn** to IP address **203.162.1.239** (server address of the software to check Bkav DNS Check error). Detailed instructions download at the following address: http://www.bkav.com.vn/DNSCheck/BkavDNSCheckGuide.html

In case the test results show an error, do the following to proceed:

1. Check which DNS system you are using is the manufacturer's software (Microsoft, Red Hat, .)

2. Error according to the instruction manual corresponding to your DNS system:

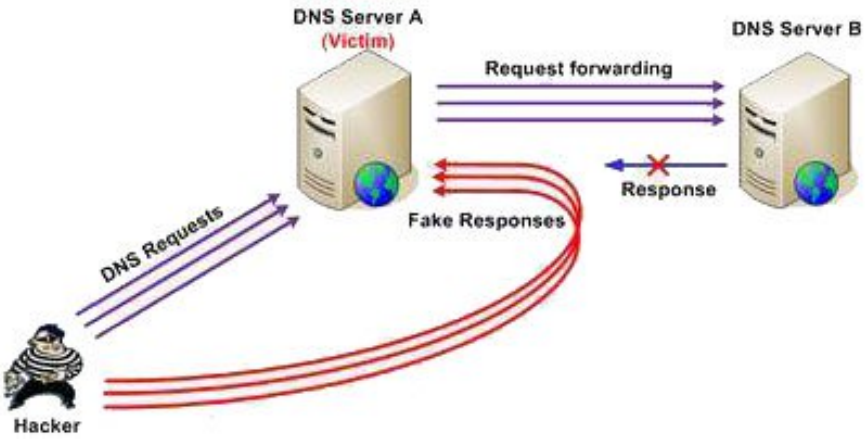
+ ***Microsoft*** : http://www.bkav.com.vn/DNSCheck/Microsoft

+ ***Red Hat*** : http://www.bkav.com.vn/DNSCheck/RedHat

+ ***FreeBSD*** : http://www.bkav.com.vn/DNSCheck/FreeBSD

+ ***Sun*** : http://www.bkav.com.vn/DNSCheck/Sun

+ ***Cisco Systems*** : http://www.bkav.com.vn/DNSCheck/Cisco



For individual users, care should be taken during this time when accessing the Internet. If you go to a familiar website but encounter an unusual phenomenon, you should immediately inform the network administrator of the agency, ISP technical support, to take timely measures. You should also fully update the operating system patches and antivirus software to avoid the risk of malicious code infection.

DNS protocol is address resolution protocol, used to map domain names (domain names) to Internet addresses (IP). According to this protocol, when the DNS server receives the request for address resolution (request) from the workstation, it will look up in the buffer (cache) and return the IP address corresponding to the domain name that the client requires. . However, if it is not found in the buffer, the DNS server will forward the resolution request to another DNS server. This is the stage that has been discovered to have a serious vulnerability and the exploit code for this vulnerability has been spread on the Internet in the past few days.

The hacker's DNS cache poisoning approach is as follows: hacker (machine H) sends a series of address resolution requests to the victim DNS server (machine A). Domain names that need to be resolved have been calculated by hackers so that server A cannot find in its buffer and must forward it to the next DNS server (machine B). Each resolution exchange between A and B is authenticated through a random TID (Transaction ID). However, the weakness here is that this TID number is only a 16 bit number (less than 65535) and all exchanges between A and B occur on a fixed port (port) of A.

The DNS cache poisoning vulnerability first appeared in the 1990s. Since then hackers have used various methods to exploit this vulnerability. This is an error in the design of the DNS protocol. For each method of exploitation, software manufacturers DNS Server has also provided patches to prevent and the problem has been fixed. However, the hacker has recently discovered a new attack method, continuing to exploit the DNS cache poisoning vulnerability.

The most important point in this method of exploiting DNS cache poisoning vulnerabilities is that hackers use subdomains (subdomains) to create valid address resolution requests. Subdomains are randomly generated in large numbers, which ensures that these domains never exist in server A's cache and force A to generate the same number of requests for forwarding to the server. B. As a result, the probability of a B-spoofing response packet generated by a hacker has a TID coinciding with the TID that machine A is waiting to be upgraded many times. The chances of successfully poisoning server A's buffer are thus enhanced.