

cert-fi

INFORMATION SECURITY REVIEW

14.10.2008

CERT-FI Information Security Review 3/2008

In the summer, information about a vulnerability in the internet domain name service (DNS) was released. If left unpatched, the vulnerability enables the misdirection of a user or direction of e-mail to false addresses by feeding forged information into the cache.

Due to the vulnerability, CERT-FI released its first warning this year. The vulnerability received major publicity on information security forums, and DNS resolvers were soon upgraded to safer versions. Therefore, the exploitation of the so-called DNS cache poisoning remained limited.

The contents of several Finnish web servers had been modified, without authorization, by exploiting the vulnerabilities of server software. The websites hosted on the hacked servers may have been defaced or used for spreading malware.

The internet address blocks of operators offering malicious content have undergone changes. Certain American internet operators have refused to provide connections to notorious entrepreneurs.

DNS vulnerability may allow misdirection of users or hijacking of email

The internet Domain Name Service is a decentralized database that translates server names and domain names into numeric IP addresses in order for the connection to be formed. E-mail delivery also takes place on the basis of the data retrieved from name servers. Domain Name Service is also known by its abbreviation, DNS.

The forgery of a single DNS record or entire domain name information would enable the misdirection of a user, hijacking of e-mail traffic or feeding malicious content to end-user computers.

Forging a so-called A record, which contains the IP address, would e.g. allow that communication to a popular website was redirected to an address appointed by the attacker. The content provided from a server controlled by the

attacker can, for example, be a piece of malware exploiting the server vulnerability or disguised as a software upgrade, website spying user information or proxy hijacking an application session.

It would be possible to misdirect e-mail messages on their way to addresses of the target company to the server controlled by the attacker by forging MX records used for directing e-mail.

If NS records listing the official name servers of a domain name are forged, all dns queries of a certain domain name could be directed to a server controlled by the attacker, which means that she or he has essentially control over any information related to the domain name.

DNS cache poisoning means loading forged data into DNS caches of DNS software

In the summer, information on vulnerabilities related to the implementation of the various parts of the DNS system was released. The vulnerabilities may expose the cache used by resolver servers, proxy components and client software to unauthorized modification by a third party. The attack technique is generally known as "*DNS cache poisoning*". The released vulnerability and its exploitation instructions provide an unforeseen way to implement the above-mentioned attack.

The vulnerability is related to how the DNS query replies are identified. The third party as an attacker tries to guess the correct identifier of the reply and thus feed the desired data to the system waiting for the answer to its DNS query. These identifiers have not been random enough in vulnerable software, so it has been possible to guess them and therefore forge the replies. By making the right guess, the attacker can feed any DNS record into the cache of the target making the query, after which it will reply to further queries with this forged data.

The attack affects only those users and information systems, which are using the "poisoned" name server and make recursive queries using the name server containing forged information. For example, if the name servers used by a broadband operator were successfully poisoned, it would have an impact on all the broadband customers of the operator in question. Respectively, the name server in the

internal network of the company would deliver false information to the company's workstations using it.

In order to fix the vulnerability, CERT-FI recommends that the software is upgraded to a version where the loading of unauthorized DNS replies has been made more difficult by improving the randomness of the query identifier. In addition, recursive DNS queries should only be allowed from the local network.

Insofar, no inbuilt verification methods of DNS query replies have been used widely, so it is theoretically still possible to forge replies. The purpose of the above-mentioned preventive measures is to reduce the risk. The introduction of the DNSSEC system has been suggested as one solution.

Vulnerable servers were searched for in Finnish networks

At the beginning of August, CERT-FI examined how well the name servers of Finnish fi-domain names were protected. A total of 4,260 name servers were tested, and their level of protection was also assessed.

It was found out that 1,180, i.e. 28 per cent of the servers examined, were poorly protected because they allow recursive queries to be made from anywhere in the internet. Of these servers, 602 appeared not to have been upgraded and therefore were potential targets to successful abuse. The root servers for fi-domain were protected as soon as the software updates were available. The servers of the biggest telecom companies were soon protected as well.

CERT-FI approached the owners of the vulnerable servers with an information bulletin. The letter suggested that the maintainers install the latest security updates to their servers, and assess whether the authoritative (primary) name server of the domain name should allow recursive queries. The survey was renewed two weeks after the information bulletins had been sent. The bulletins were found to have had a minor impact on the total number of vulnerable servers, but there were still 491 servers which appeared vulnerable.

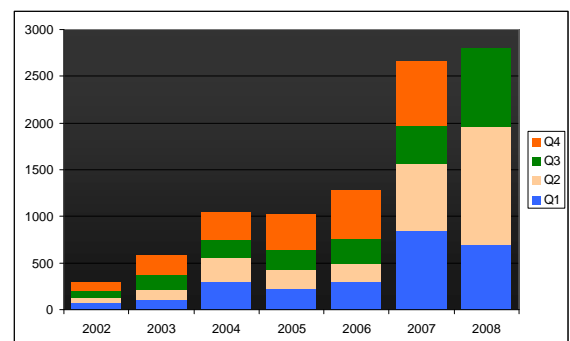
The vulnerability was exploited in Finland

A case where a DNS vulnerability had been exploited by directing the attack to the DNS of the company's internal network was reported to CERT-FI

The attacker was successful in loading a new A record with long expiration date (TTL) into the cache of a name server located in the internal network of the company. The name information related to the A record was of such a form that the company's web browsers automatically used it for web proxy auto-discovery.

The configuration server controlled by the attacker directed the web browser to use the proxy controlled by the attacker. Thus, all network communication related to web browsing was routed through the IP address defined by the attacker.

In this case, the IP address pointed to a hacked web server located in the company's internal network, which was used for spying the users' Windows domain names and passwords.



By the end of September this year, slightly more cases were recorded in the CERT-FI incident handling management system than the total number of cases reported the year before.

Attacks to websites

Vulnerabilities found in web servers continue to be exploited. Only a minor part of the hacked servers reported to CERT-FI were located in Finland.

This spring, a phenomenon where websites vulnerable to SQL injection attacks are used for spreading malware, was first discovered on a large scale. This activity continued during the summer. Also vulnerable Finnish sites have occasionally been harnessed for misuse.

SQL injection results from insufficient input validation and back-end database protection. It is then possible to store information on the vulnerable website or a database used by the website by injecting an appropriate SQL statement to the back-end database via the web page. It is also possible to gain confidential information from the database in the background of a vulnerable site.

Also, *Remote File Inclusion* attacks have been regularly discovered. An error in the configuration of web applications implemented by PHP programming language allows an attack where the attacker can inject manipulated program code to be processed by the server. The attacks have made use of several ready-made malware packages that can be used for sending spam, for example.

Vulnerabilities found in popular web content management systems, discussion forums and blog software allow the attacker, in some cases, to reset or discover the administrative password for web application management. This allows the attacker to manipulate the content of the website using the vulnerable application platform. Vulnerabilities have also been used in other attacks against Finnish web servers. In these attacks, servers have, for example, been harnessed as platforms of phishing sites.

Finnish server spread malware repeatedly

CERT-FI received reports of a Finnish web server constantly user for spreading malware. Because there had been vulnerabilities in the server that were not rectified, new malware could be uploaded again on the server after the administrators had cleaned it up. In this case, the investigations on the role of the server maintainer are pending.

Malware can be disguised as anti-virus software

Recently, several malware have tried to make users install themselves by disguising as anti-virus software. The websites of the malware have been built to resemble the sites of companies that provide free versions of virus protection software in addition to the commercial versions. Some of these sites are found only when the site is accessed via a search engine.

It may often be more efficient to spread the malware by luring the user to install it by himself rather than exploiting software vulnerabilities as an infection method of the malware.

The conflict in Georgia had no impact on Finnish networks

The armed conflict in Georgia also involved activism and network attacks in information networks. The attacks were targeted at news sites and politically-charged targets of lesser importance to the activities of the information society. The attacks had no direct impact on the functionality or safety of Finnish networks.

Changes in build-ups of malicious network traffic

Malicious activity in the internet, such as the spreading of malware, the data storage servers of malware and the command and control servers of botnet networks need server resources in order to be effective.

There are some hosting service providers whose network addresses have significantly more malicious content or traffic than the average provider. The reason for the build-up of malicious content can be that the company has an indifferent attitude towards the quality of the services provided by its customers. For some, this may even be a competitive advantage sustained on purpose.

Intercage from San Francisco was an ill-famed service provider whose network segments were often connected with malware cases. A domain name provider called *Estdomains* has been its customer, and has been connected with several domain names used for malicious purposes.

Due to the pressure from the information security community, operators who had provided network connections to *Intercage*, disconnected it at the end of September. *Estdomains*

continues its activities by using the connections of other service providers. Some of the network addresses used by Intercage have been transferred to other service providers.

Previously, the focus has also been on the activities of *Russian Business Network* from St. Petersburg. RBN disappeared from the network in 2007. Several service providers of the same type as Intercage and RBN are also currently active.

Certain service providers are so concentrated on the provision of malicious content that if traffic from Finnish networks is directed to addresses used by these providers it is reasonable to suspect that there is a malware infection in the workstation trying to access these addresses. Corresponding clusters of malicious services have not been found in Finland or other Nordic countries.

More possibly prevalent vulnerabilities will be released soon

Recently, vulnerabilities in several TCP protocol stacks have received a lot of publicity. According to public information, the vulnerabilities could facilitate a denial-of-service attack with low traffic volumes. CERT-FI coordinates the assessment of the effects of the vulnerability, eventual repair procedures and release together with software manufacturers and the finder of the vulnerability. Additional information on the vulnerability will be released in accordance with the best practices of vulnerability release process.

CERT-FI contacts per item	1-3/2008	4-6/2008	7-9/2008	Total	1-9/2007	Change
Interview	17	29	21	67	62	+8%
Vulnerability or threat	39	232	52	323	40	+708%
Malware	460	727	532	1719	1286	+34%
Guidance	64	87	92	243	280	-13%
Preparation for attack	32	27	12	71	3	+2267%
Data break-in	14	88	45	147	43	+242%
Denial-of-service attack	15	26	31	72	49	+47%
Other information security problem	10	11	12	33	21	+57%
Social Engineering	47	36	44	127	167	-33%
Total	698	1263	841	2802	1969	+42%

Reports made of vulnerabilities or threats have increased significantly from the previous year. The growth of the number of reports is affected by website vulnerabilities actively searched for, which can also be seen in the figures for realized data break-ins.