More than 70,000 Memcached servers are still capable of being hacked remotely

Nothing in this world is 100% safe, from the real world to cyberspace. The vulnerabilities are troublesome but worse than that, we didn't update the patches in time.

At the end of last year, Cisco's Talos research team found that there are three important remote code execution vulnerabilities (RCE) in Memcached on websites that can help hackers attack users' machines, including There are also sites like Facebook, Twitter, YouTube, Reddit.

Memcached is an open source system that stores objects and data that are accessed multiple times to speed up access. It is used to speed up web applications (eg PHP websites) by reducing the burden on the database. It's been nearly 8 months since Memcached developers released a patch for these three RCE vulnerabilities (CVE-2016-8704, CVE-2016-8705 and CVE-2016-8706) but thousands of servers run Memcached applications. still not updated, allowing attackers to easily steal sensitive data remotely.

Many Memcached servers are still vulnerable

Researchers at Talos do Internet scans at two times, late February and July to see how many servers are running unpatched versions. The results are surprising.

Scan results in February:

1. General server on Internet 107,786
2. Vulnerable server 85.121
3. The server is vulnerable and requires verification 23,707

The five countries with the most vulnerable servers are the United States, followed by China, Britain, France and Germany.

Scan results in July:

1. Total server on Internet 106.001
2. Vulnerable server 73,403
3. Vulnerable server and need of 18,012 authentication

After comparing the results of the two scans, the researchers found that only 2,958 servers were vulnerable to the scan in February before patching before July, while the rest were still vulnerable to remote hacking.

Data theft and ransomware hazards

It is very important for organizations to ignore this patch, and Talos researchers warn that this vulnerable Memcached will be the target of ransomware attacks similar to the one that attacked. MongoDB database at the end of December.

Although unlike Mongo DB, Memcached is not a database, but it still contains sensitive information and interferes with the service, which can lead to other obstacles on independent service.

The error on Memcached will allow hackers to replace the saved content with malicious content to change the website content, create phishing sites, extort money, poison the link, attack the victim computer, bring hundreds of millions of users. into a dangerous state.

> 'As more and more computer worms exploit vulnerabilities, this needs to be alarmed with administrators around the world,' the researchers concluded. 'Untreated weaknesses when exploited can affect organizations worldwide, affecting serious work. These systems should be patched immediately to minimize risks'.