

Nginx DoS İstismar Kodu

written by Mert SARICA | 17 May 2013

7 Mayıs tarihinde Nginx'in resmi web sayfasında, Greg MacManus tarafından nginx v1.3.9 ve 1.4.0 sürümlerinde tespit edilen bellek taşması güvenlik zafiyeti (CVE-2013-2028) için bir yama yayınlandığı belirtilmişti. Can sıkıntısı nedeniyle bu zafiyet üzerinde yaptığım 1 saatlik bir araştırmada, bu zafiyeti istismar eden ve nginx web sunucusunu hizmet dışı bırakan bir istismar kodu hazırladım.

Kali ve Windows XP işletim sistemleri üzerinde denediğim ve Exploit-DB'ye gönderdiğim istismar koduna buradan ulaşabilirsiniz.

The image is a collage of screenshots demonstrating a Denial of Service (DoS) attack on Nginx. It is divided into three main sections:

- Top Left:** A terminal window showing the execution of a DOS POC script for Nginx CVE-2013-2028. The script sends multiple requests to a target IP, causing a memory overflow. The output shows the script successfully sending 5 requests.
- Top Right:** A SecureCRT window displaying the output of the 'top' command on the target system. The output shows high CPU usage (99.7%) and a large number of tasks (145 total), indicating a denial of service.
- Middle:** A SecureCRT window showing the Nginx configuration file being modified. The configuration is set to listen on a specific IP address (192.168.1.63) and serve a specific directory.
- Bottom Left:** A terminal window showing the execution of the DOS POC script on a Windows XP system. The script successfully sends 5 requests, causing a denial of service.
- Bottom Right:** A Windows Task Manager window showing the processes running on the system. The 'nginx.exe' process is highlighted, showing it is consuming 99% of the CPU, which is the result of the DoS attack.

Not: Exploit-DB ve Packetstorm'a dosyaları gönderirken CVE-2013-2028 yerine CVE-2013-2070 olarak göndermişim, doğrusu CVE-2013-2028 olacaktır.
I submitted the POC code with wrong CVE (CVE-2013-2070) to Exploit-DB & PacketStorm so the correct one is CVE-2013-2028.