

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 illustrating 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. The script repeatedly sends requests to a target, causing a denial of service. The output shows the script running successfully for 5/5 attempts.
- Top Right:** A system monitor window (top) showing system statistics, including CPU usage (99.7%) and memory usage (416440 used). Below it, a terminal window shows the Nginx configuration file being modified to include the attack script.
- Bottom Left:** A terminal window showing the execution of the DOS POC script on a Windows XP system. The script successfully sends requests to the target, causing a denial of service.
- Bottom Right:** A Windows Task Manager window showing the 'nginx.exe' process consuming 99% of the CPU, indicating a successful denial of service 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.