

# 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 displays three screenshots illustrating the Nginx DoS exploit:

- Top Left:** A Kali Linux terminal window showing the execution of the exploit code. The code sends a series of requests to a target server, causing a memory overflow. The terminal output shows the exploit being successful, with the server crashing.
- Top Right:** A Kali Linux terminal window showing the system's status after the exploit. The terminal output shows the system's memory usage and the status of various processes, including nginx.
- Bottom Left:** A Windows XP terminal window showing the exploit's effect on the target server. The terminal output shows the server crashing and displaying an error message.
- Bottom Right:** A Windows Task Manager screenshot showing the system's performance after the exploit. The CPU usage is at 100%, and the nginx.exe process is running with high memory usage.

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.