Exploit Arama Yöntemi

Herhangi bir sunucunun exploit'ini aramak istediğimizde google arama motoruna aşağıdaki anahtar kelimeler girilir

Google Arama Kutusu:

Windows Server 2016 exploits
Windows Server 2012 exploits
…

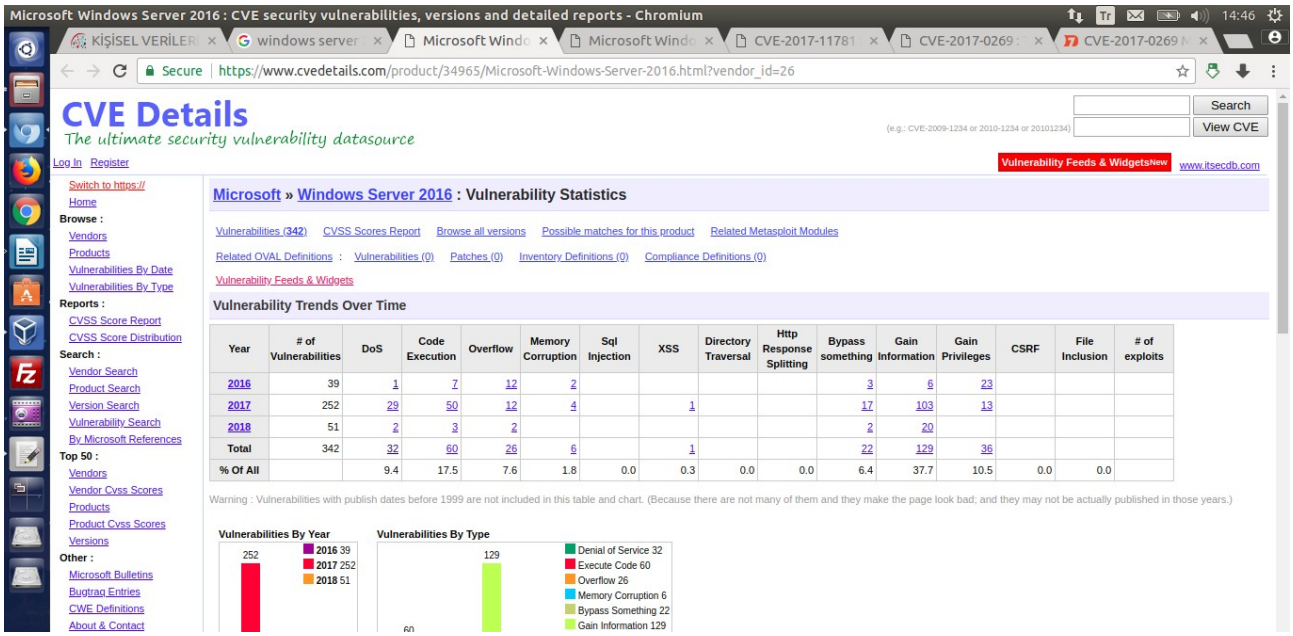
Bu aramalar sonucunda CVE Details veritabanına götüren linke tıklanır.

https://www.cvedetails.com/product/34965/Microsoft-Windows-Server-2016.html?vendor_id=26

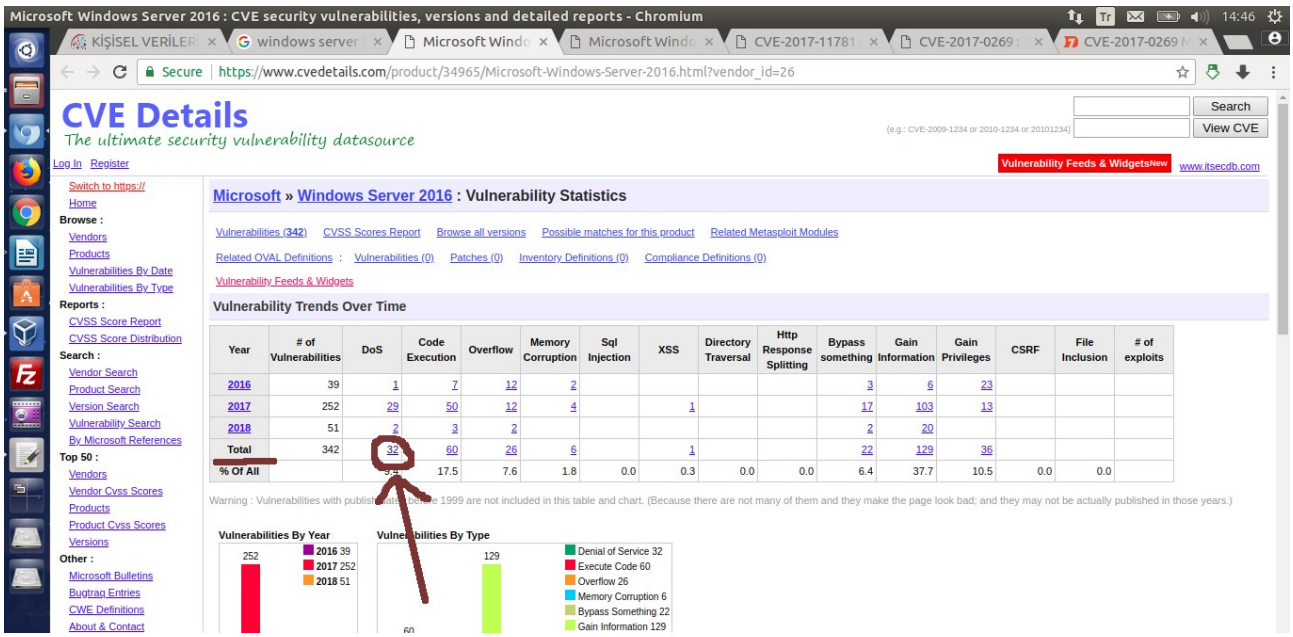
https://www.cvedetails.com/product/23546/Microsoft-Windows-Server-2012.html?vendor_id=26

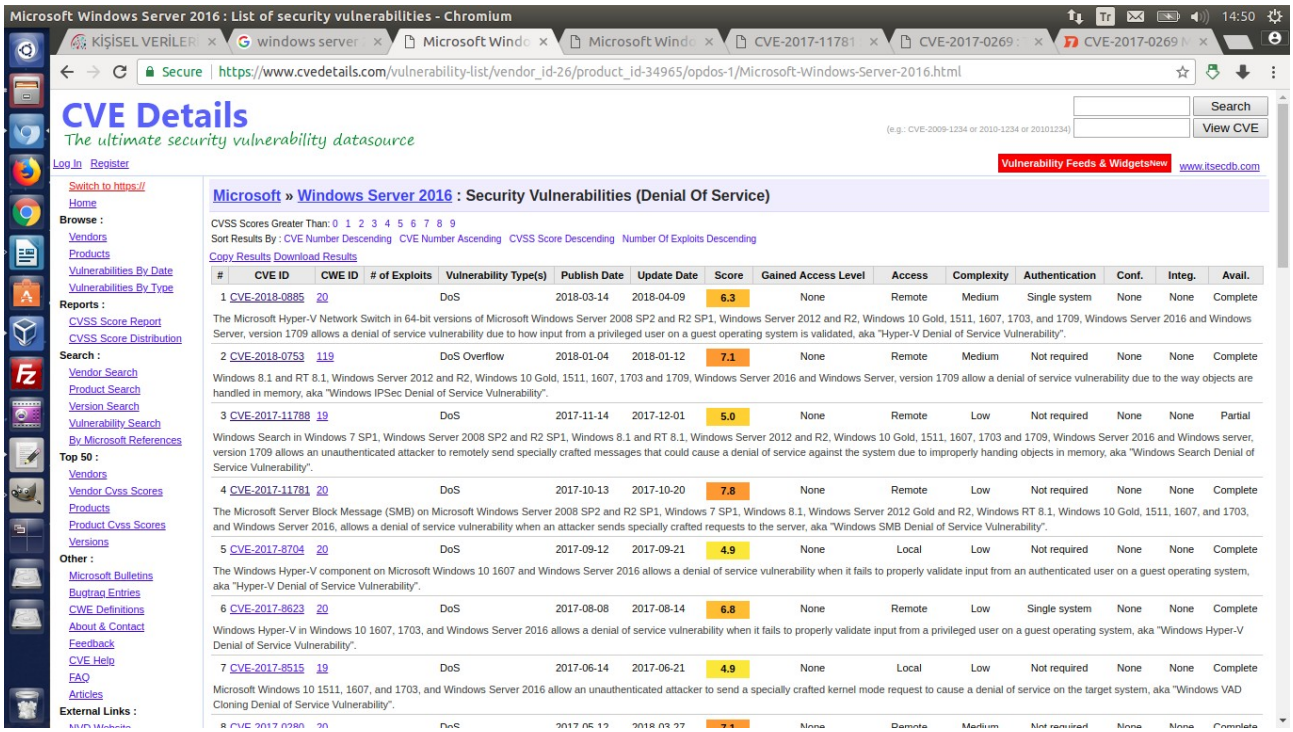
…

CVEDetails veritabanında (örneğin yukarıdaki linklerden birinde) aşağıdaki gibi bir sayfa bizi karşılar.

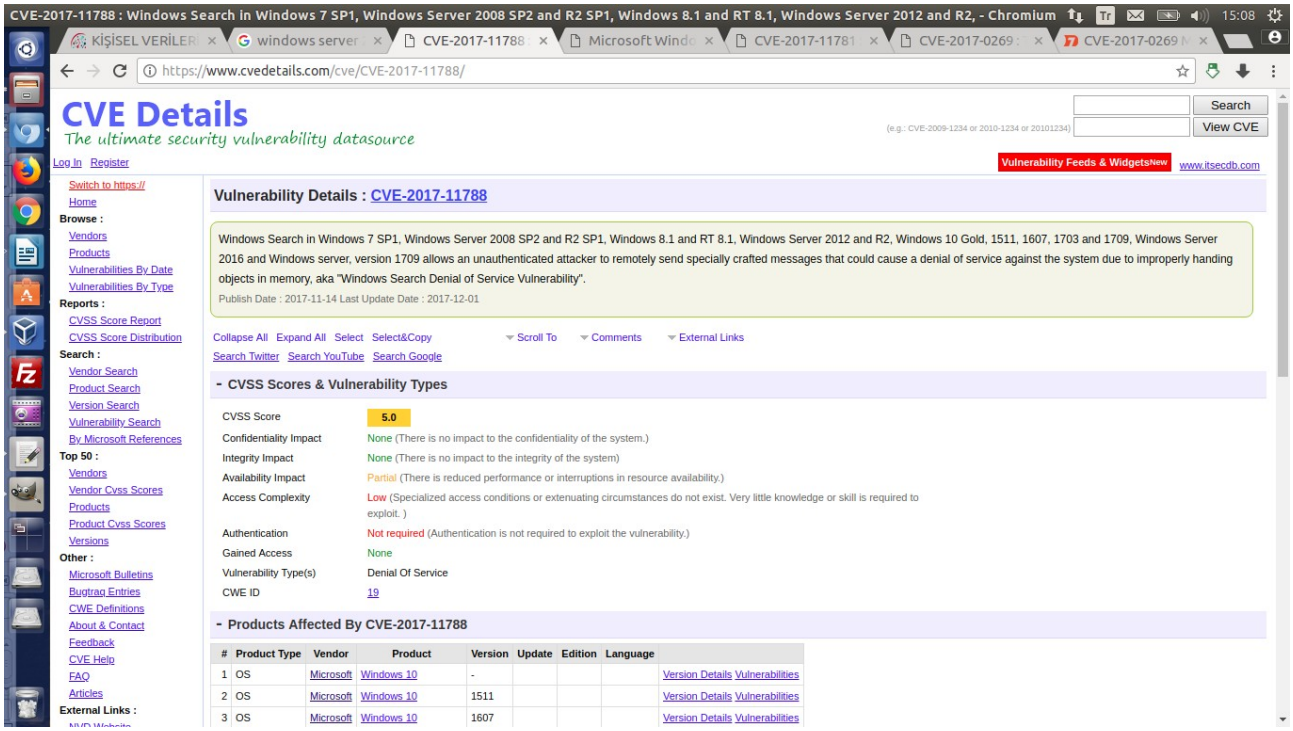


Örneğin bu sayfada Window Server 2016'ya ait tüm zafiyetler kategorize edilerek sıralanmıştır. DoS, Code Execution, Overflow, … vs. Bu zafiyetlerin altında ise satır satır yıllara göre çıkan zafiyetlerin sayısı gösterilmiştir. Total satırına gelip oradaki rakama tıkladığımızda (örn; DoS'un Total satırındaki rakama tıkladığımızda) Windows Server 2016'ya ait bu zamana kadar çıkmış tüm DoS zafiyetleri ekrana gelir.

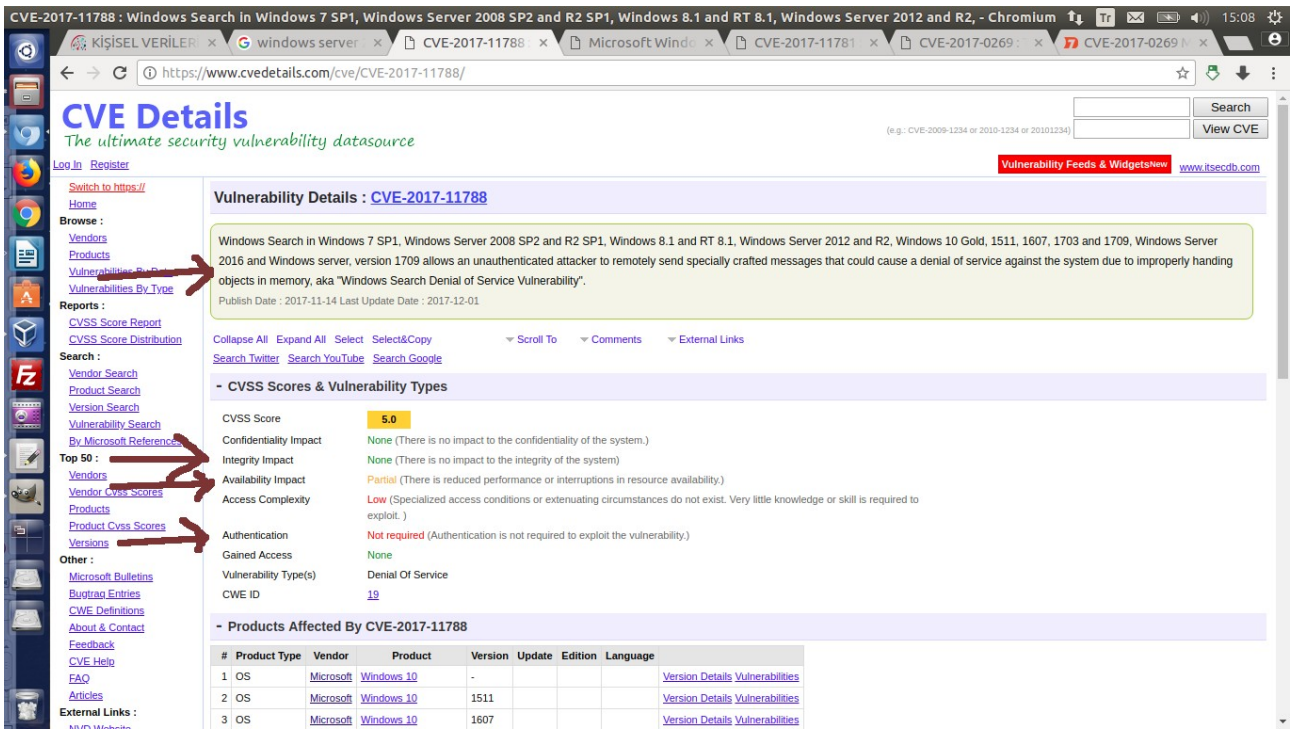


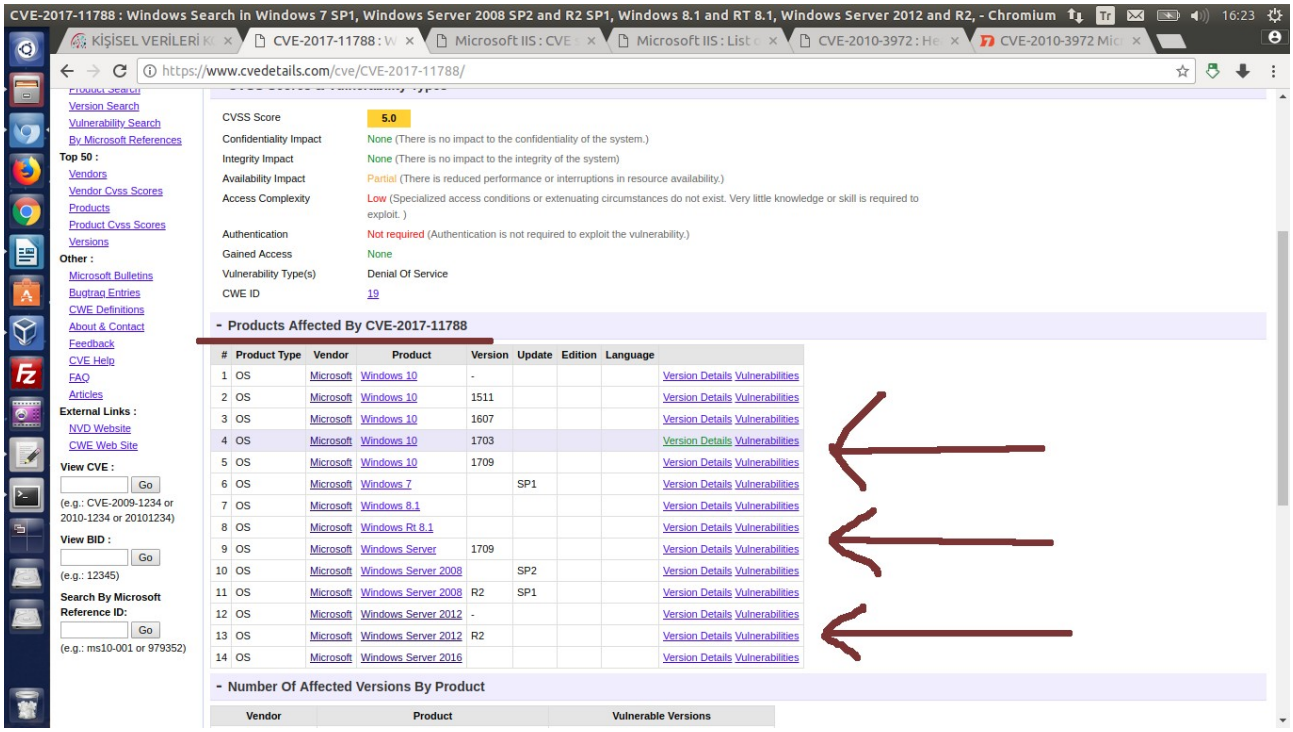


Görüldüğü üzere Windows Server 2016 'nın DoS zafiyetlerini görüntülemekteyiz. Zafiyetlere sırasıyla tıkladığımızda aşağıdaki gibi bir sayfa bizi karşılar.

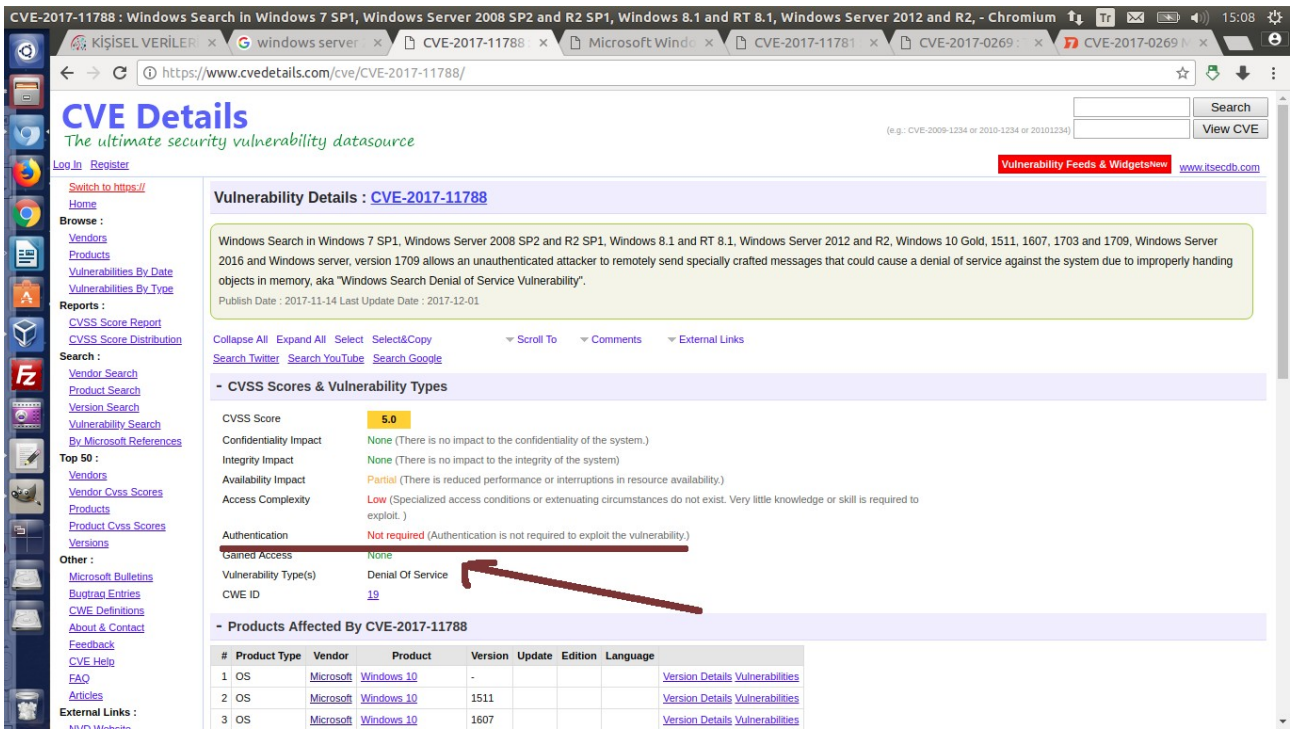


Bu sayfada zafiyetin açıklaması, zafiyetin exploit edilebilmesi için authentication'a gerek var mı yok mu şartı (Authentication), exploitation işleminin sistemin bütünlüğüne zarar verip vermediğinin bilgisi (Integrity Impact), exploitaiton işleminin sistemin erişilebilirliğine zarar verip vermediğinin bilgisi (Availability Impact) ve zafiyetten etkilenen yazılımların listesi (products affected by cve-xxx) gösterilir.

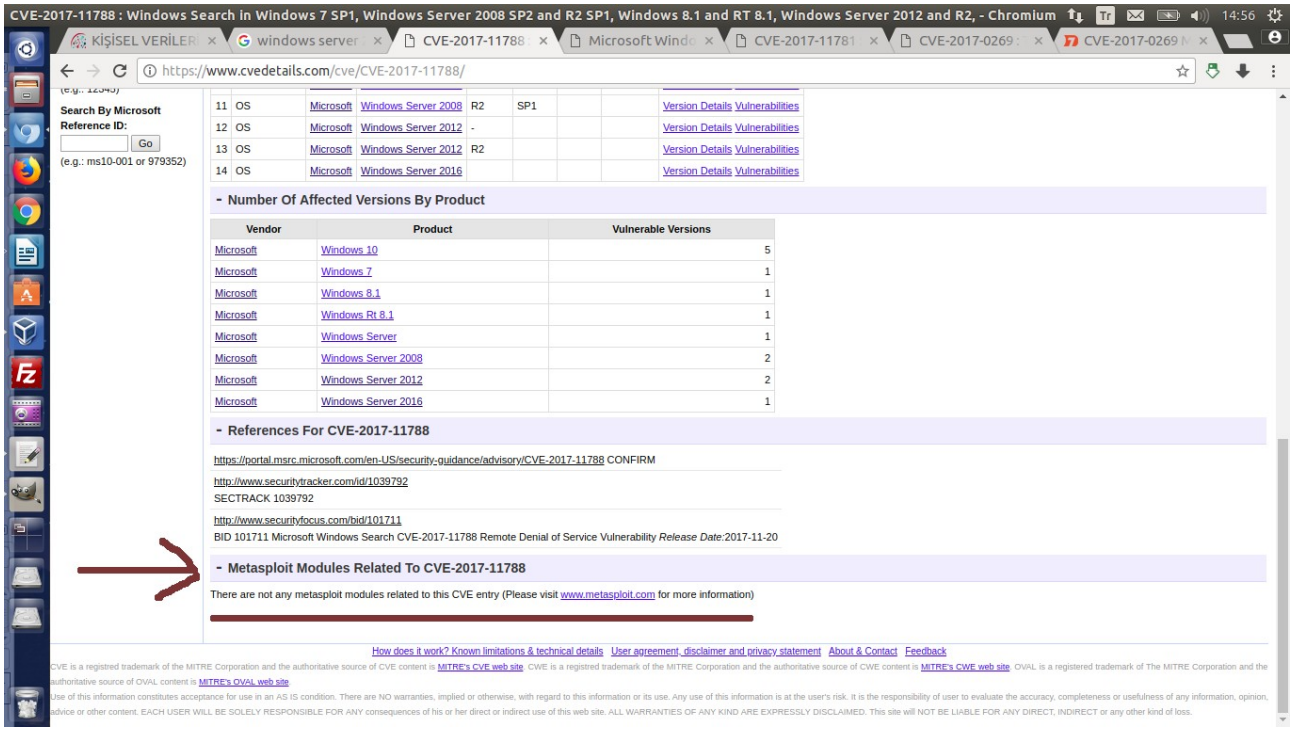




Zafiyetin exploit edilebilmesi için authentication'ın gerekli olmayışı bizim avantajımızadır. Çünkü böylece credential'lara sahip olmadan exploitation yapabiliriz. Aşağıda exploitation yapmak için authentication'a ihtiyaç olmayan bir zafiyet gösterilmiştir.



Seçtiğimiz zafiyet sayfasının en altında ise zafiyetin metasploit'te bir exploit modülüne sahip olup olmadığı bilgisi gösterilir



Görüldüğü üzere seçtiğimiz zafiyetin metasploit'te bir modülü yokmuş. CVE Details veritabanının güncellenmemesi ihtimaline karşı google arama moturuna zafiyetin CVE kodunu (örneğin bu zafiyet için CVE-2017-11788 kodunu) girip rapid7 sitesinden metasploit modülü gelmiş mi (gösterilmekte mi) bakabiliriz.