CVE Nedir ve Kullanımı

MITRE firması 1999 yılında CVE adını verdiği bir sistem başlatmıştır. Açılımı Common Vulnerabilities and Exposures olan CVE ürünlerdeki kamuya yansımış açıklıkların numaralandırıldığı bir standarttır. 2005 yılında ABD devleti Ulusal Açıklık Veritabanı'nı (National Vulnerability Database - NVD'yi) başlatmıştır. ABD devletinin başlattığı Ulusal Açıklık Veritabanı MITRE firmasının hizmeti olan CVE veritabanı kayıtlarını xml / json feed'leri ile alır, kullanır ve üzerine ilave bazı ekstra bilgiler ekleyerek ulusal cve veritabanı hizmeti olarak sunar.

MITRE'nin CVE'si ve ABD devleti Ulusal Açıklık Veritabanı (NVD) iki ayrı oluşum olsa da ikisi de ABD devleti Yurt Güvenliği Departmanı'nın Siber Güvenlik ve Altyapı Güvenliği Ajansı'nca fonlanmaktadır. MITRE firması CVE sistemini ABD devleti Siber Güvenlik ve Altyapı Güvenliği Ajansı adına yürütmektedir ve ABD devlet ajansı adına çalıştırılmaktadır.

MITRE firması CVE listesini idare eder. CVE girdileri özettirler. Teknik detaylar, riskler, etkiler, ve yamalar hakkında bilgi içermezler. Bu gibi bilgiler farklı veritabanlarında bulunabilir. Örneğin; MITRE'nin kayıtlarını kullanan, ek bilgiler ilave etmiş ABD devleti Ulusal Açıklık Veritabanı'nda (NVD'de) olduğu gibi.

Bir güvenlik açığının CVE girdisi haline girmesi sıklıkla organizasyonlar veya açık kaynak topluluklarının üyeleri tarafından açıklığın MITRE'ye gönderilmesiyle gerçekleşir. Bazen de MITRE firması doğrudan cve girdisi oluşturur.

CVE girdilerini yazanlar CVE Numaralandırma Otoriteleri tarafından atanırlar. Yaklaşık 100 kadar CVE Numaralandırma Otoritesi vardır. Bunlar arasında IBM, Cisco, Oracle, RedHat, Microsoft,..., çeşitli güvenlik şirketleri ve araştırma organizasyonları vardır. MITRE bu girdi yazan otoritelerin yanında ayrıca doğrudan CVE girdi yazımında bulunabilmektedir.

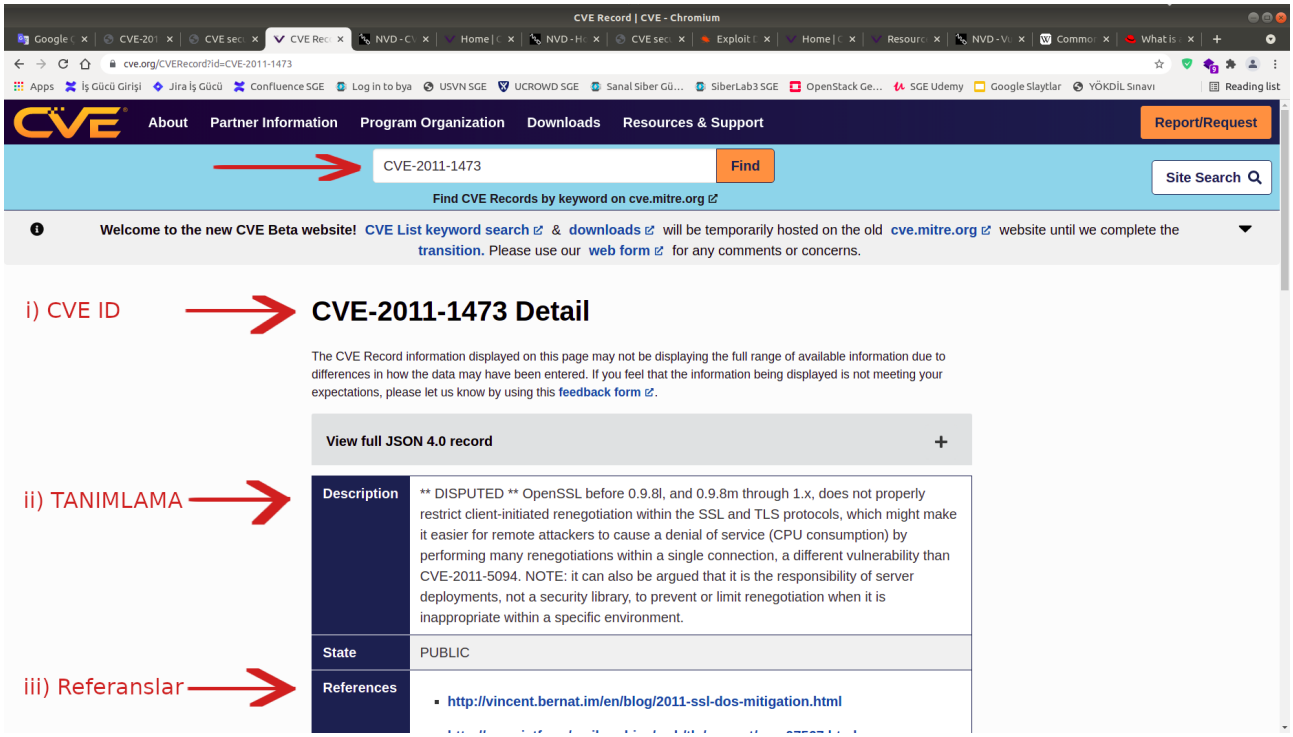
Aşağıda MITRE'nin veritabanını kullanarak CVE veritabanı hizmeti sunan çeşitli web siteleri verilmiştir.

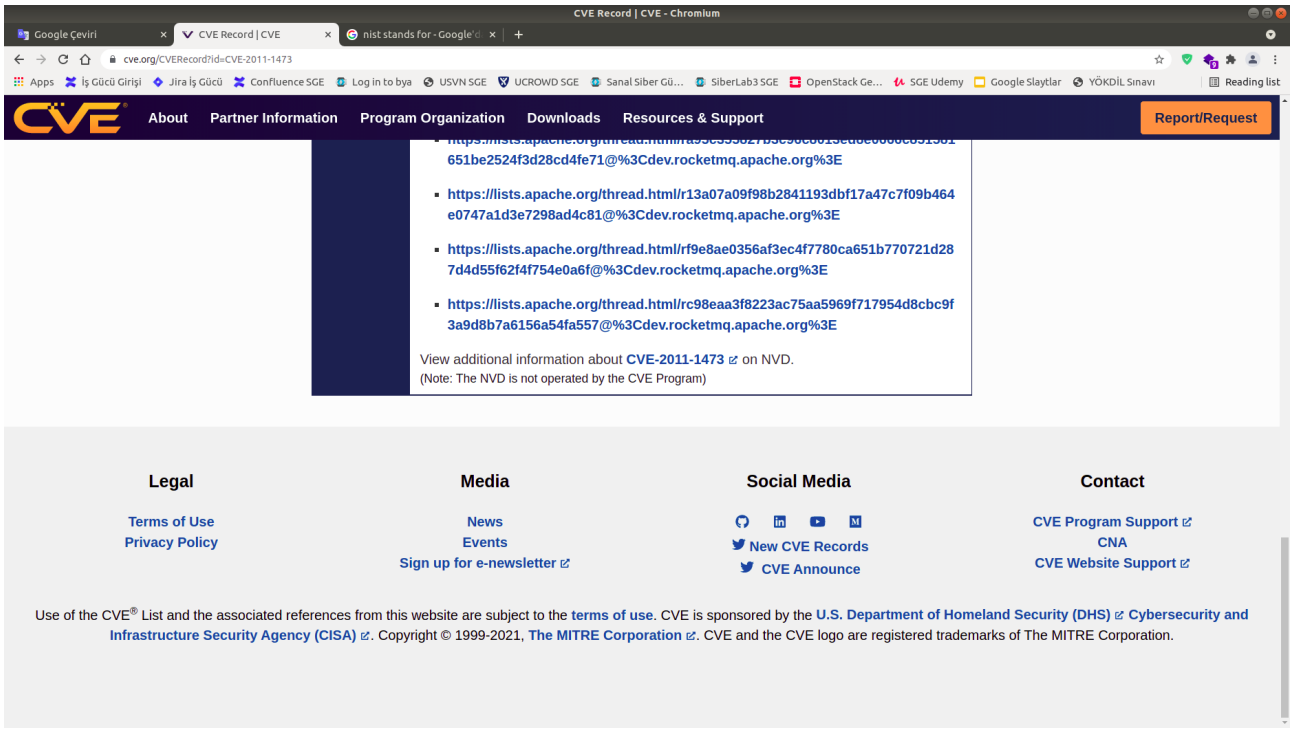
```
// MITRE Firmasının Sunduğu CVE Veritabanı
https://cve.mitre.org/ (mevcut)
https://www.cve.org/ (yenisi)

// MITRE Firmasının Kayıtlarını Kullanan ABD
// Ulusal Açıklık Veritabanı'nın (NVD'nin) CVE
// Veritabanı
https://nvd.nist.gov/

// MITRE Firmasının Kayıtlarını Kullanan RedHat
// Firmasının Sunduğu CVE Veritabanı
https://access.redhat.com/security/security-updates/#/cve

// ABD Ulusal Açıklık Veritabanı (NVD) Kayıtlarını
// Kullanan (Dolaylı Yoldan MITRE Firmasının Ka-
// yıtlarını Kullanmış Olan) CVEDetails Web Sitesi-
// nin Sunduğu CVE Veritabanı
https://www.cvedetails.com/
```

Bu siteler MITRE firmasının CVE kayıtlarını xml ve json feed'leri ile alarak ve bazısı çeşitli ekstra eklemelerde bulunarak kullanmaktadırlar. Bu şekilde MITRE'nin sunduğu cve veritabanını web sayfalarında sunmaktadırlar.

CVE Nasıl Kullanılır?

CVE girdileri bir CVE ID'ye, özet bir tanımlamaya ve referans linklerine sahiptirler. Aşağıda MITRE firmasının cve sitesindeki (https://www.cve.org/) bir cve girdisi şablonu gösterilmiştir.





MITRE’nin bu CVE sayfa şablonunda yer alan bölümler şu şekildedir:

i) CVE ID

CVE ID bölümü ürünlerde çıkan açıklıklara verilen kimlik numarasını sunar. Kimlik numaraları CVE-YEAR-NUMBER şeklinde standardize bir numaralandırma ile sunulur.

ii) Description

Tanımlama bölümü numaralandırılan ilgili ürün açıklığının özet bir bilgisini sunar.

> Özet Bilgi Hakkında Yol Haritası
>
> Yukarıdaki resimde gösterilen örnek CVE-2011-1473 id’li açıklığın özet bilgisinde OpenSSL’in 0.9.8l ve öncesi, ve ayrıca 0.9.8m’den 1.x’e kadarki sürümlerinde SSL/TLS’teki renegotiation’ın uygun kısıtlanmadığı bildirilmiş ve bu durumun saldırganlara CPU tüketimi ile servis dışı bırakma saldırıları yapabilmelerine imkan tanıdığı söylenmiş. Bu özet bilgiden yola çıkarak belirtilen açıklığı sömürme uygulamasını açıklığın tanımlamasında belirtilen uygulama ve sürümlerinde tatbik edebileceğimizi anlayabilir ve belirtilen uygulama ve sürümlerinde ne tür bir saldırı yapılabilir olduğunu (yani vektör türünü) görebiliriz. Buradan hareketle farklı web sitelerinde açıklığın sömürülmesi üzerine ve tool üzerine araştırma yapılabilir (örn; cve referanslar son bölümündeki linkler incelenebilir) ve sanal bir vm’de cve tanımlamasında söylenen uygulamanın (örn; bu açıklık özelinde openssl’in) açıklıklı sürümü kurularak bulunan bir tool’la bu açıklığı sömürme uygulaması yapılabilir.
>
> Not: Bu resimde gösterilen CVE-2011-1473 id’li açıklığı SSL/TLS Renegotation açıklığı olarak ifade edilir ve OpenSSL zafiyeti üzerinden DoS saldırısı yapmayı sağlar. Bu CVE açıklığı hakkında açıklamalar, açıklığın nasıl sömürüldüğü bilgileri ve tool ile açıklığı sömürme uygulaması için bkz. Paketleme İçin Gözden Geçirilecekler / SSL,TLS DoS Saldırısı ile Apache Web Sunucuları Servis Dışı Bırakma.docx

Tanımlama bölümü özet bilgisinden önce ** DISPUTED ** veya ** RESERVED ** şeklinde etiketler yer alabilir. Özet bölümünün başında DISPUTED (Tartışmalı) etiketinin yer alması ilgili ürün satıcısı veya ilgili ürün otoritesinin açıklığın geçerliliğine itiraz ettiği anlamına gelir. Bu itiraz durumu olduğunda ilgili CVE girdisi, özet bilgisinin en başına ** DISPUTED ** eklenmek suretiyle etiketlenir (bkz. Yukarıdaki resimdeki cve açıklığı gibi). Özet bölümünün başında RESERVED (Rezerve Edildi) etiketi yer alması ise ilgili açıklığın nihai halde paylaşımı için daha fazla detaya ihtiyaç olduğu anlamına gelir. Eğer açıklık eksiklikler nedeniyle yayınlamak üzere uygun değil şeklinde kesinleşirse REJECTED yapılır.

iii) Referans

Referans bölümü ise ilgili ürün açıklığı hakkında tavsiyeler, güvenlik çözümleri, ve tool’lar hakkında bilgiler paylaşan web site url adresleri sunar.

Ekstra

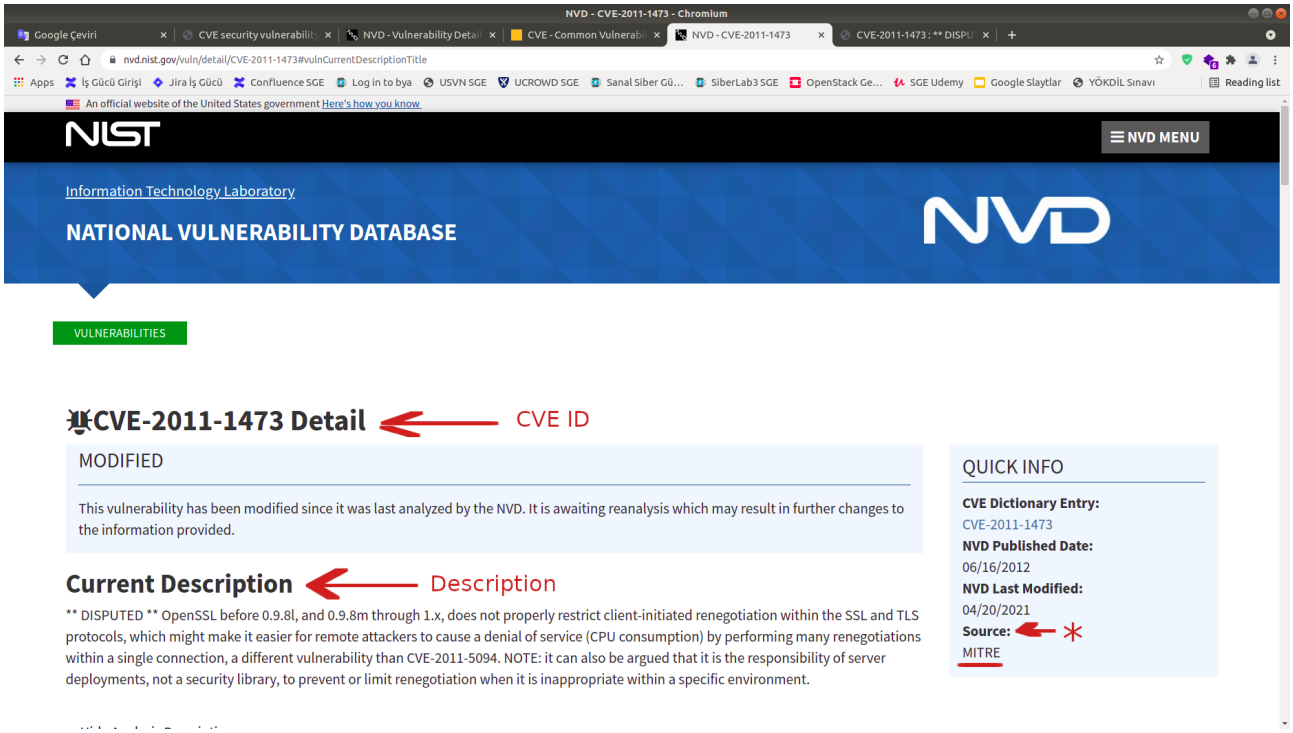
MITRE'nin cve veritabanını sunan çeşitli web sitelerinden bazıları cve girdilerindeki cve id'si, özet bilgisi ve referans linklerine ek olarak ekstra bilgiler ilave edebilmektedirler. Örneğin ABD devleti Ulusal Açıklık Veritabanı (NVD)'nin nvd.nist.gov web sitesi ve farklı bir oluşum olan cvedetails.com web sitesi gibi:

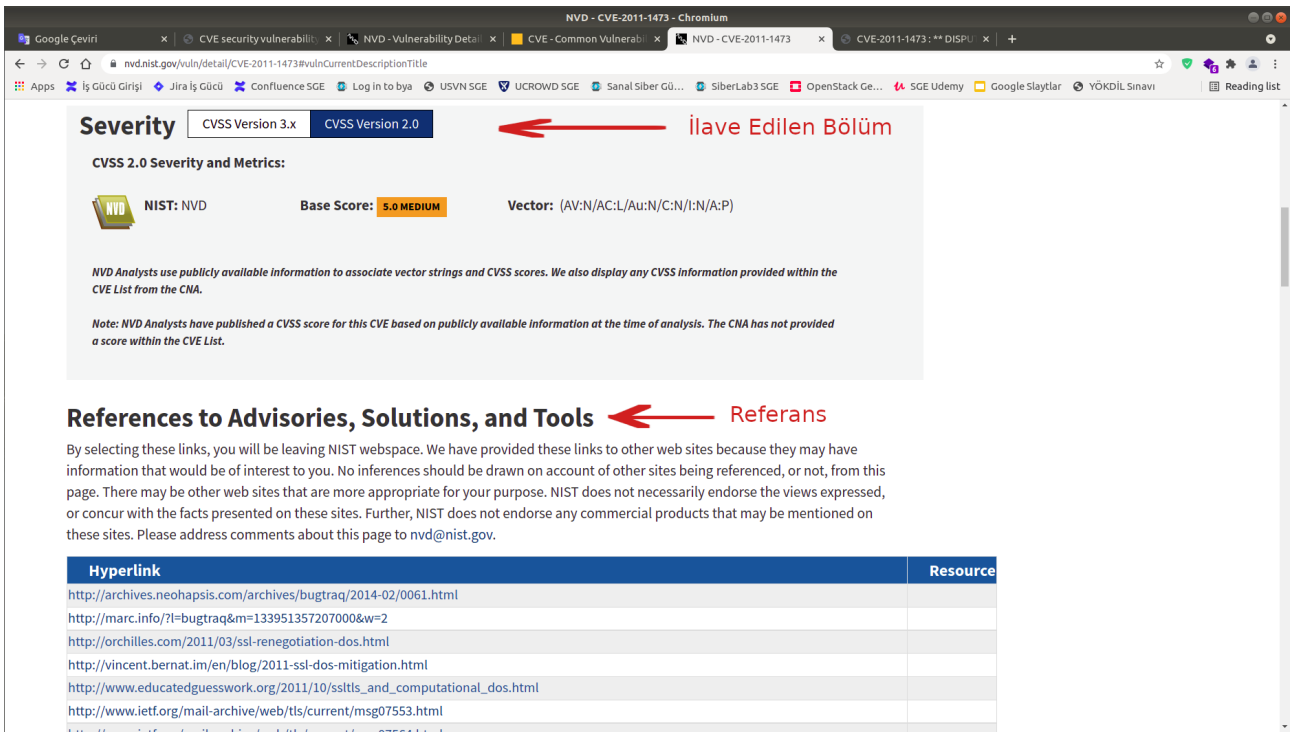
a) nvd.nist.gov

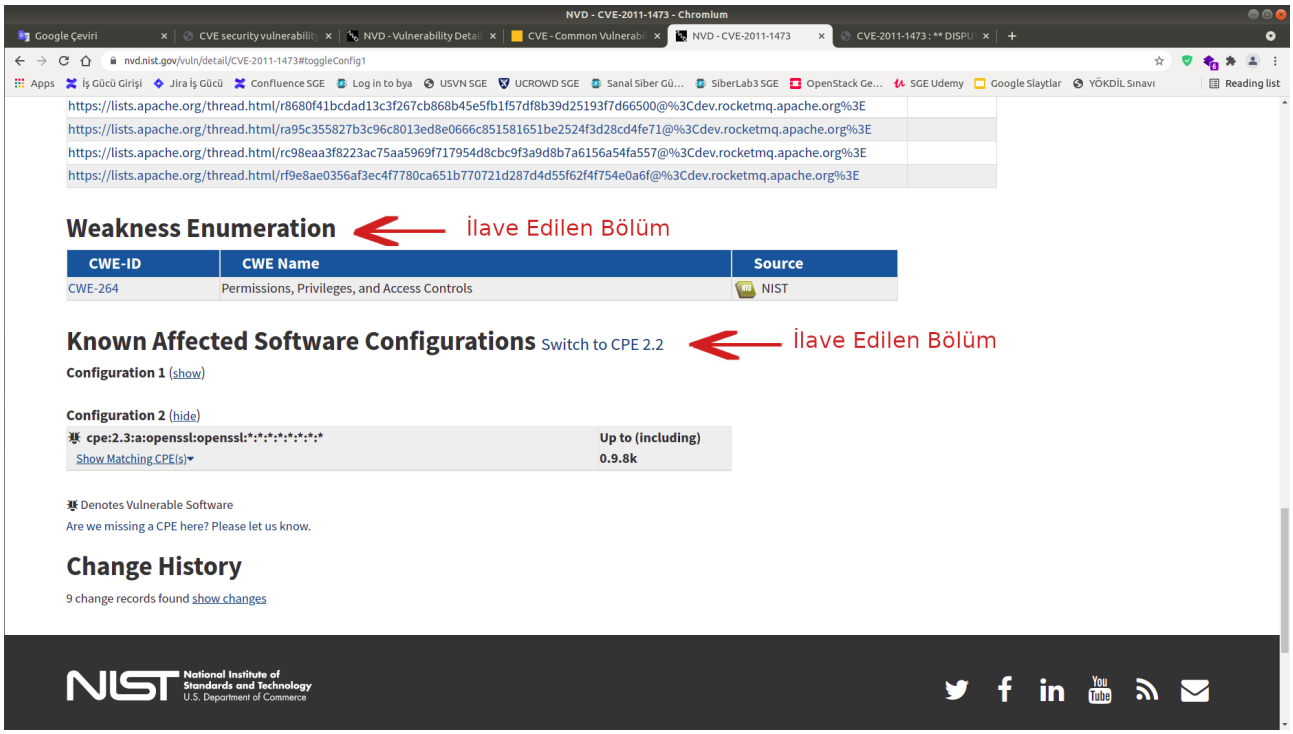
ABD devleti Ulusal Açıklık Veritabanı resmi web sayfası (https://nvd.nist.gov/), MITRE'den çekilen cve girdilerine ait id, özet ve referans şeklindeki üç bilgi unsuruna CVSS skorunu, CWE kodunu, CVE ID açıklığından etkilenen ürün ismini ve sürümlerini ilave etmektedir.

> CVSS Skoru Nedir?
>
> CVSS (Common Vulnerability Scoring System) skoru açıklıkların bir formülle 0.0 ile 10.0 arası aralıkta değerlendirildiği bir puanlama sistemidir. Çok sayıda parametrenin (atak karmaşıklık seviyesi, yetki gerekli mi, gizliliği ne seviyede etkiliyor, bütünlüğü ne seviyede etkiliyor, erişilebilirliği ne seviyede etkiliyor, açıklığı kapama seviyesi… v.b.) değerlendirmeye katılmasıyla skorlama yapılır. İlgili kullanılan formülü görmek veya değerlendirme hesaplaması için cvss v3 calculator kullanılabilir.

Aşağıdaki resimde ABD devleti Ulusal Açıklık Veritabanı resmi web sayfasından bir cve açıklık sayfası örneği paylaşılmıştır.







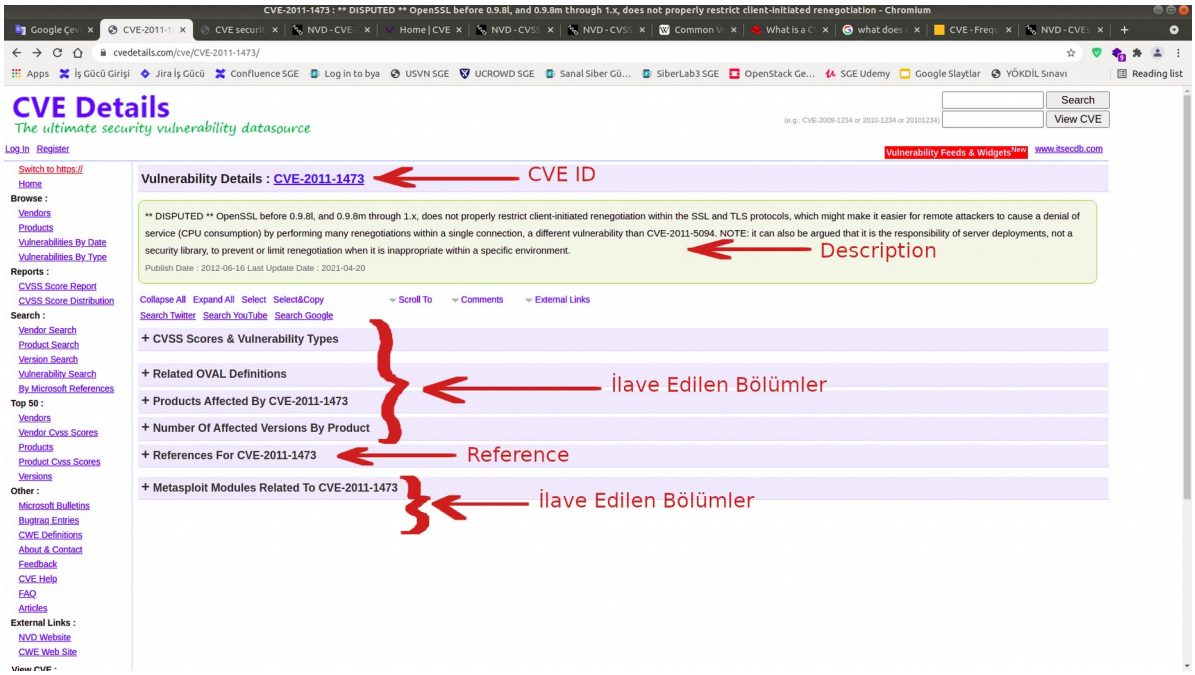
Not: Bu resimde gösterilen CVE-2011-1473 id'li örnek açıklık SSL/TLS Renegotation açıklığı olarak ifade edilir ve OpenSSL zafiyeti üzerinden DoS saldırısı yapmayı sağlar. Bu CVE açıklığı hakkında açıklamalar, açıklığın nasıl sömürüldüğü bilgileri ve tool ile açıklığı sömürme uygulaması için bkz. Paketleme İçin Gözden Geçirilecekler / SSL,TLS DoS Saldırısı ile Apache Web Sunucuları Servis Dışı Bırakma.docx

Görüldüğü gibi MITRE'nin cve kayıtlarındaki cve id'si, özet bilgisi, referans bilgisi şeklinde olan üç unsuruna NVD'de ilave unsurlar eklemesi yapılmıştır.

b) www.cvedetails.com

www.cvedetails.com web sitesi ise yine cve kayıtları sunar. Anasayfasındaki ifadelere göre ABD devleti Ulusal Açıklık Veritabanı resmi web sitesinin (https://nvd.nist.gov/'in) sunduğu xml feed'lerini alarak cve girdilerini edinir. Daha doğru bir ifadeyle Amerikan Ulusal Açıklık Veritabanı (NVD) kayıtları MITRE'den aldığından dolayı Cvedetails web sitesi dolaylı yoldan MITRE'den cve kayıtlarını edinir. Bu edindiği cve girdilerindeki id, özet ve referans şeklindeki üç bilgi unsuruna CVSS (Common Vulnerability Scoring System) skorunu, açıklık türü hakkında ek bilgileri, OVAL adı verilen bazı tanımlamaları, CVE ID açıklığından etkilenen ürünleri, CVE ID açıklığından etkilenen ürünlerin sürümlerini, ve CVE ID açıklığı için Metasploit Modülü var mı yok mu bilgisini ilave etmektedir. Cvedetails web sitsi adının da belirttiği gibi cve'yi detaylı (yani donatılmış ek bilgilerle) sunmaktadır.

Aşağıdaki resimde Cvedetails web sayfasından bir cve açıklık sayfası örneği paylaşılmıştır.



> Not: Bu resimde gösterilen CVE-2011-1473 id'li örnek açıklık SSL/TLS Renegotation açıklığı olarak ifade edilir ve OpenSSL zafiyeti üzerinden DoS saldırısı yapmayı sağlar. CVE ID açıklığında metasploit modülü var mı bölümünde metasploit modülü olmadığı ifade edilmektedir. Metasploit modülü yoktur, fakat bu saldırı thc-ssl-dos adında bir hacker grubunun geliştirdiği araçla yapılabilmektedir. Sonuç olarak bu metasploit bölümünden tool araştırmasına gidilebilir.

Görüldüğü gibi MITRE'nin cve girdilerindeki cve id'si, özet bilgisi, referans bilgisi şeklinde olan üç unsuruna Cvedetails'de ilave unsurlar eklemesi yapılmıştır.

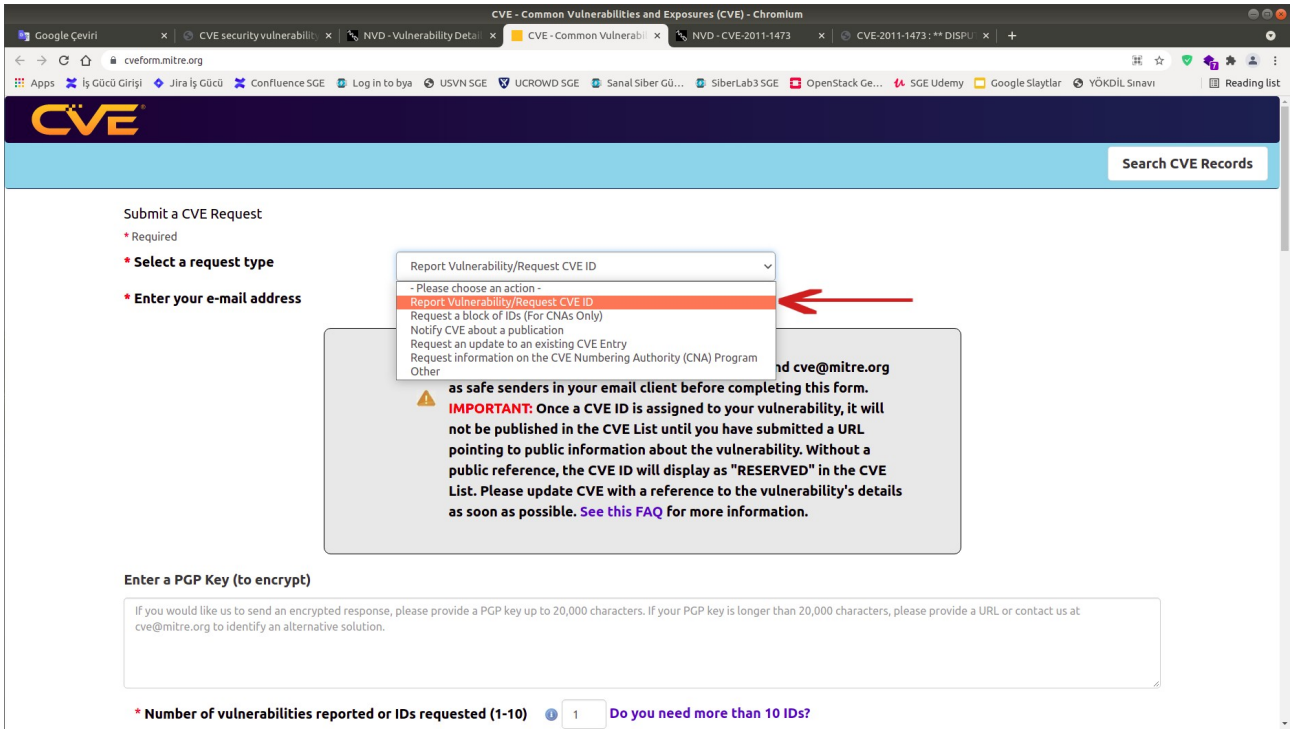
Ekstra 2

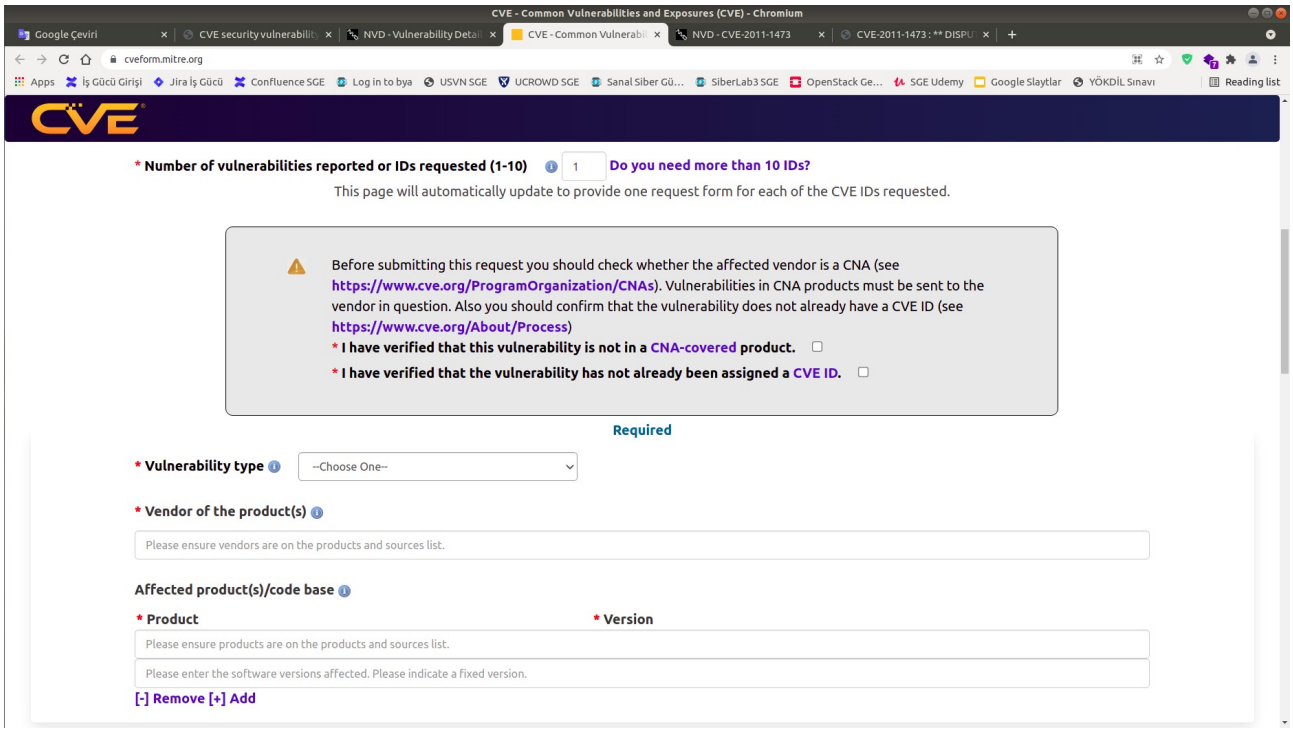
Siber güvenlikçi olarak bir üründe açıklık bulduğumuzda ve CVE olarak yayınlanmadığını fark ettiğimizde bu açıklık için MITRE firmasına CVE ID oluşması adına talepte bulunabiliriz.

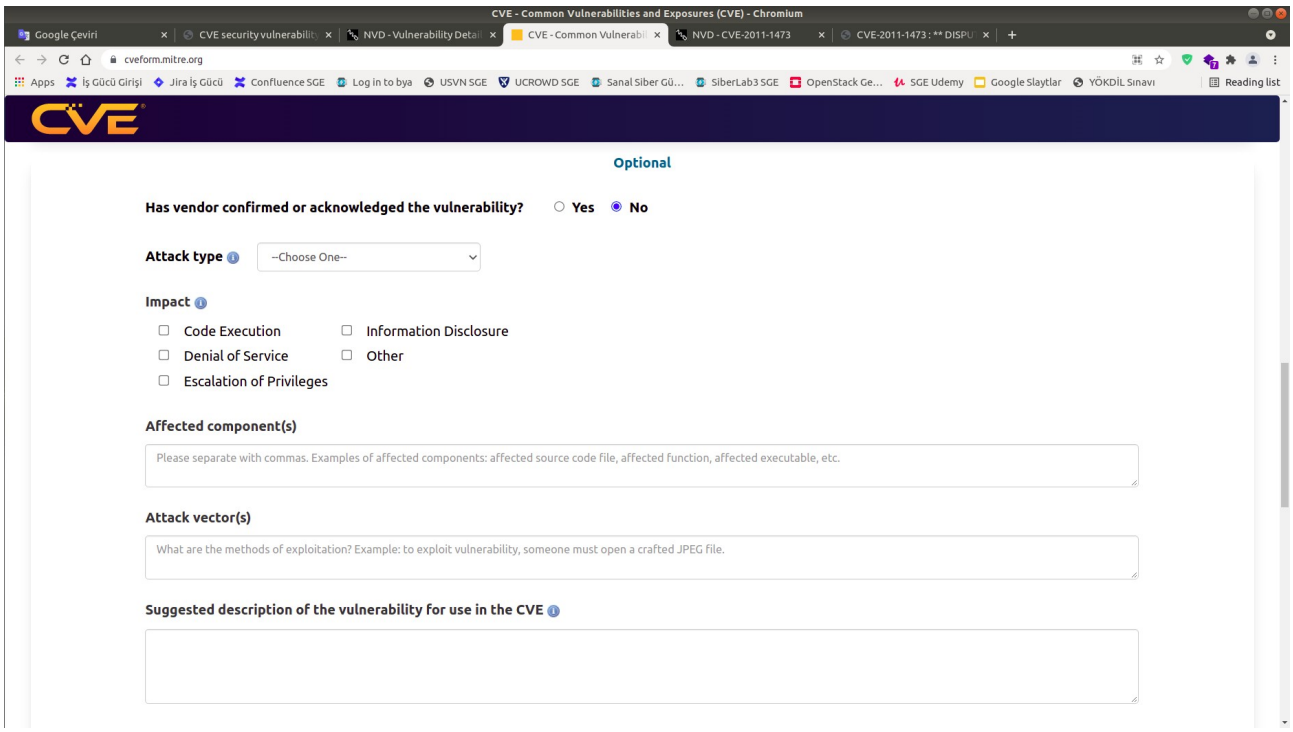
Talep Formu:

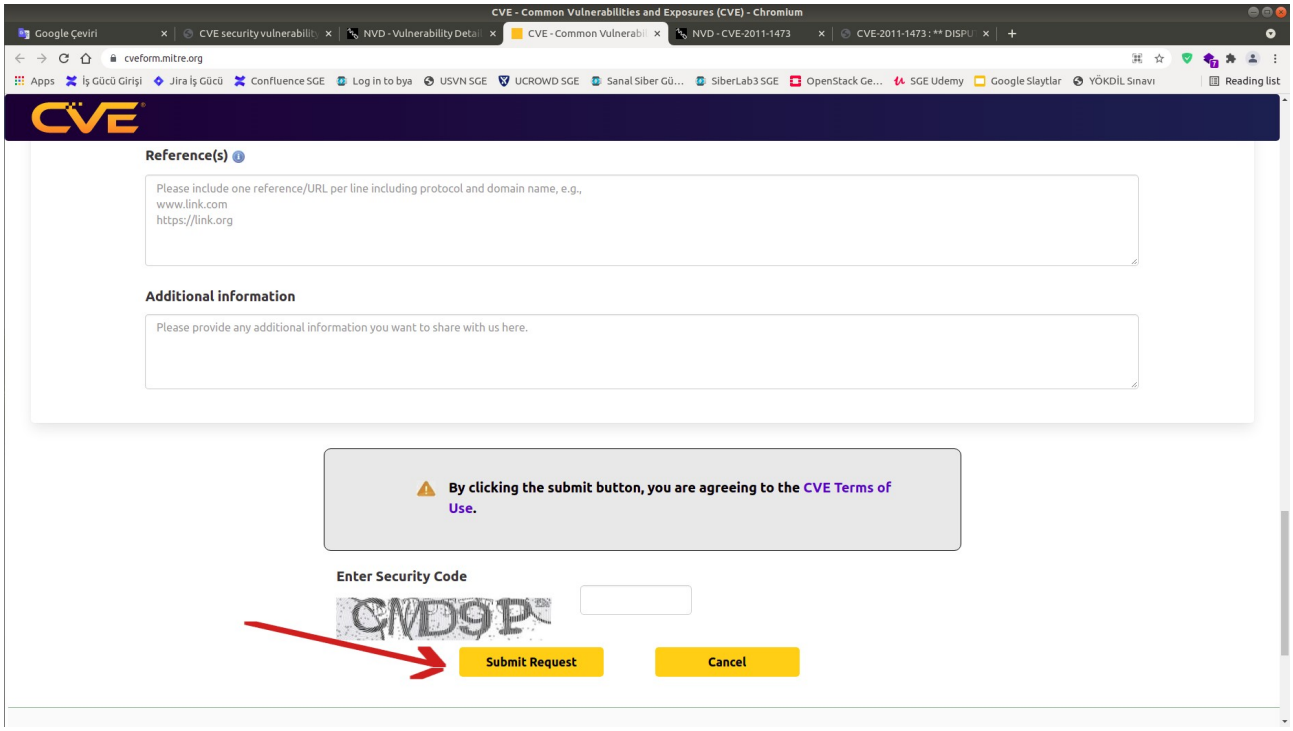
https://cveform.mitre.org/

Çıktı:









Cve veritabanında bulunmayan kendi bulduğumuz bir açıklık için bir CVE ID bu yolla oluşturabiliriz. Açık kaynak topluluklar ve organizasyonlar bu yolla kendi buldukları açıklıklarını MITRE firmasına başvuru formu üzerinden bildirmektedirler ve MITRE firması da açıklığı geçerli bulursa cve veritabanına kaydetmektedir. CVE kaydı oluşmuş bu açıklığı MITRE firmasının cve kayıtlarını kullanan diğer tüm cve veritabanı web siteleri de MITRE'den feed'leri otomatize ve senkronize bir şekilde aldıklarından dolayı aynı anda web sitelerinde sunmaktadırlar.

Kaynaklar:

https://www.redhat.com/en/topics/security/what-is-cve#:~:text=Security%20Data%20API%3F-,Overview,at%20least%20one%20CVE%20ID.

https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

https://cve.mitre.org/about/cve_and_nvd_relationship.html

https://nvd.nist.gov/general/cve-process

https://nvd.nist.gov/vuln/vulnerability-detail-pages

https://cveform.mitre.org/

https://www.cvedetails.com/

https://access.redhat.com/security/security-updates/#/cve

https://cve.mitre.org/

https://www.cve.org/