

## 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 özetirler. 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-

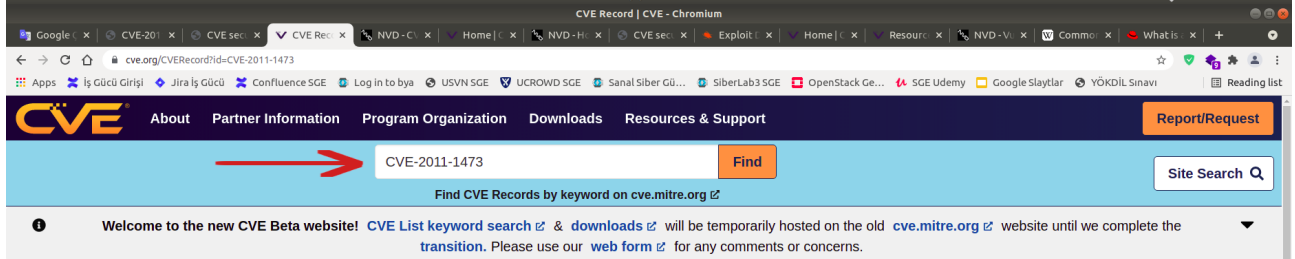
// nin Sunduğu CVE Veritabanı

<https://www.cvedetails.com/>

Bu siteler MITRE firmasının CVE kayıtlarını xml ve json feed'leri ile alarak ve bazısı çeşitli ekstra eklemelerde bulunarak kullanılmaktadır. 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.



### i) CVE ID → CVE-2011-1473 Detail

The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered. If you feel that the information being displayed is not meeting your expectations, please let us know by using this [feedback form](#).

View full JSON 4.0 record +

### ii) TANIMLAMA →

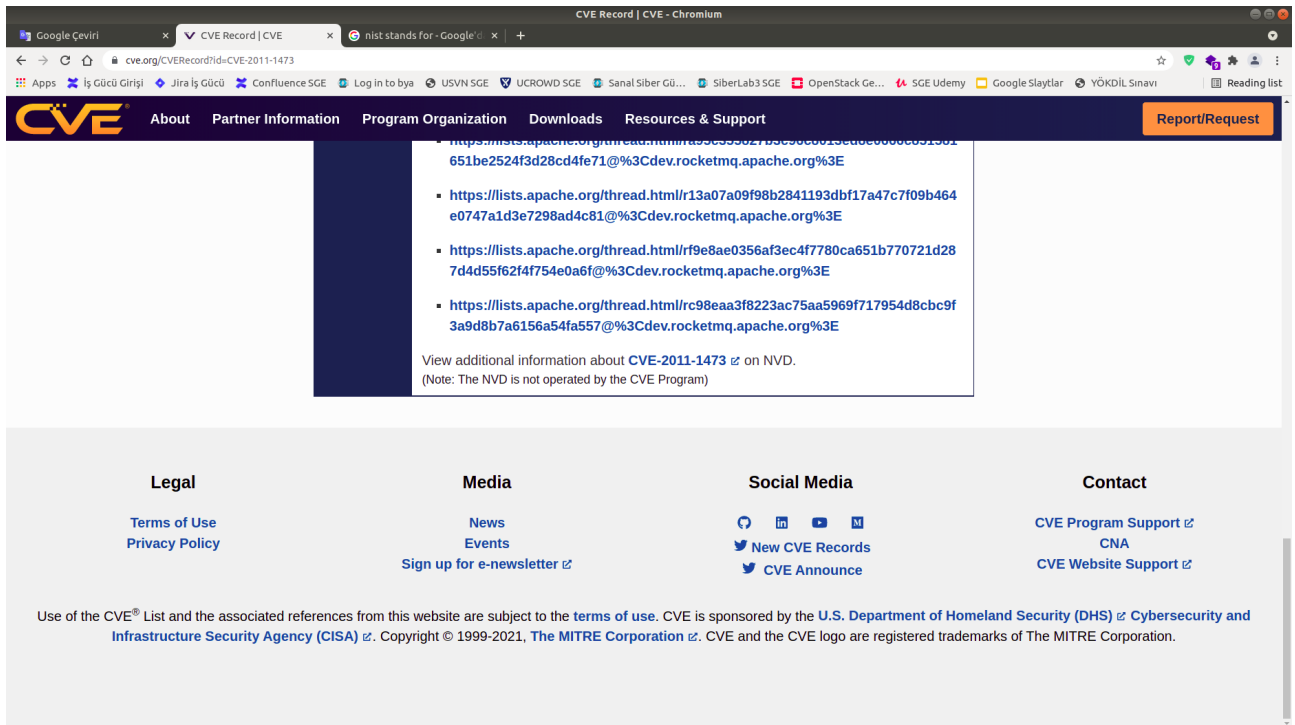
**Description** \*\* DISPUTED \*\* OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

### iii) Referanslar →

**State** PUBLIC

**References**

- <http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html>



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 Renegotiation 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](https://nvd.nist.gov) web sitesi ve farklı bir oluşum olan [cvedetails.com](https://cvedetails.com) web sitesi gibi:

### a) [nvd.nist.gov](https://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.

The screenshot shows the NVD website interface. At the top, there's a navigation bar with the NIST logo and 'NATIONAL VULNERABILITY DATABASE' text. Below that, a 'VULNERABILITIES' section is highlighted. The main content area is titled 'CVE-2011-1473 Detail'. It includes a 'MODIFIED' section with a note about reanalysis. The 'Current Description' section contains a detailed description of the vulnerability. The 'QUICK INFO' section provides key details: CVE Dictionary Entry (CVE-2011-1473), NVD Published Date (06/16/2012), NVD Last Modified (04/20/2021), and Source (MITRE). Red arrows point to the CVE ID, the 'Description' label, and the 'Source' field in the 'QUICK INFO' section.

NVD - CVE-2011-1473 - Chromium

Severity CVSS Version 3.x CVSS Version 2.0 **İlave Edilen Bölüm**

CVSS 2.0 Severity and Metrics:

NIST: NVD Base Score: 5.0 MEDIUM Vector: (AV:N/AC:L/Au:N/C:N/I:N/A:P)

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The CNA has not provided a score within the CVE List.

References to Advisories, Solutions, and Tools **Referans**

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
<a href="http://archives.neohapsis.com/archives/bugtraq/2014-02/0061.html">http://archives.neohapsis.com/archives/bugtraq/2014-02/0061.html</a>	
<a href="http://marc.info/?l=bugtraq&amp;m=133951357207000&amp;w=2">http://marc.info/?l=bugtraq&amp;m=133951357207000&amp;w=2</a>	
<a href="http://orchilles.com/2011/03/ssl-renegotiation-dos.html">http://orchilles.com/2011/03/ssl-renegotiation-dos.html</a>	
<a href="http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html">http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html</a>	
<a href="http://www.educatedguesswork.org/2011/10/sslts_and_computational_dos.html">http://www.educatedguesswork.org/2011/10/sslts_and_computational_dos.html</a>	
<a href="http://www.ietf.org/mail-archive/web/tls/current/msg07553.html">http://www.ietf.org/mail-archive/web/tls/current/msg07553.html</a>	

NVD - CVE-2011-1473 - Chromium

Weakness Enumeration **İlave Edilen Bölüm**

CWE-ID	CWE Name	Source
CWE-264	Permissions, Privileges, and Access Controls	NIST

Known Affected Software Configurations **İlave Edilen Bölüm**

Switch to CPE 2.2

Configuration 1 (show)

Configuration 2 (hide)

⚔ cpe:2.3:a:openssl:openssl:\*:\*:\*:\*:\* Up to (including) 0.9.8k

Show Matching CPE(s)

⚔ Denotes Vulnerable Software

Are we missing a CPE here? Please let us know.

Change History

9 change records found [show changes](#)

NIST National Institute of Standards and Technology U.S. Department of Commerce

Twitter Facebook LinkedIn YouTube RSS Email

Not: Bu resimde gösterilen CVE-2011-1473 id'li örnek açıklık SSL/TLS Renegotiation 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 unsura NVD'de ilave unsurlar eklenmesi yapılmıştır.

## b) www.cvedetails.com

www.cvedetails.com web sitesi ise yine cve kayıtları sunar. Anasayfasındaki ifadelerle 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 sitesi adının da belirttiği gibi cve'yi detaylı (yani donatılmış ek bilgilerle) sunmaktadır.

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

The screenshot shows the CVE Details website for CVE-2011-1473. The page title is "Vulnerability Details : CVE-2011-1473". The main content area contains the following sections:

- Vulnerability Details : CVE-2011-1473** (CVE ID)
- Description**: "\*\* DISPUTED \*\* OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment. Publish Date : 2012-06-16 Last Update Date : 2021-04-20"
- CVSS Scores & Vulnerability Types** (İlave Edilen Bölümler)
- Related OVAL Definitions** (İlave Edilen Bölümler)
- Products Affected By CVE-2011-1473** (İlave Edilen Bölümler)
- Number Of Affected Versions By Product** (İlave Edilen Bölümler)
- References For CVE-2011-1473** (Reference)
- Metasploit Modules Related To CVE-2011-1473** (İlave Edilen Bölümler)

Not: Bu resimde gösterilen CVE-2011-1473 id'li örnek açıklık SSL/TLS Renegotiation 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 eklenmesi 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:

Submit a CVE Request

- \* Required
- \* Select a request type
- \* Enter your e-mail address

Report Vulnerability/Request CVE ID

- Please choose an action -

- Report Vulnerability/Request CVE ID
- Request a block of IDs (For CNAs Only)
- Notify CVE about a publication
- Request an update to an existing CVE Entry
- Request information on the CVE Numbering Authority (CNA) Program
- Other

and cve@mitre.org

as safe senders in your email client before completing this form.  
**IMPORTANT:** Once a CVE ID is assigned to your vulnerability, it will not be published in the CVE List until you have submitted a URL pointing to public information about the vulnerability. Without a public reference, the CVE ID will display as "RESERVED" in the CVE List. Please update CVE with a reference to the vulnerability's details as soon as possible. See this FAQ for more information.

Enter a PGP Key (to encrypt)

If you would like us to send an encrypted response, please provide a PGP key up to 20,000 characters. If your PGP key is longer than 20,000 characters, please provide a URL or contact us at cve@mitre.org to identify an alternative solution.

\* Number of vulnerabilities reported or IDs requested (1-10) 1 Do you need more than 10 IDs?

\* Number of vulnerabilities reported or IDs requested (1-10) 1 Do you need more than 10 IDs?

This page will automatically update to provide one request form for each of the CVE IDs requested.

Before submitting this request you should check whether the affected vendor is a CNA (see <https://www.cve.org/ProgramOrganization/CNAs>). Vulnerabilities in CNA products must be sent to the vendor in question. Also you should confirm that the vulnerability does not already have a CVE ID (see <https://www.cve.org/About/Process>)

- \* I have verified that this vulnerability is not in a CNA-covered product.
- \* I have verified that the vulnerability has not already been assigned a CVE ID.

Required

\* Vulnerability type --Choose One--

\* Vendor of the product(s)

Please ensure vendors are on the products and sources list.

Affected product(s)/code base

\* Product \* Version

Please ensure products are on the products and sources list.

Please enter the software versions affected. Please indicate a fixed version.

[-] Remove [+] Add

CVE - Common Vulnerabilities and Exposures (CVE) - Chromium

Google Çeviri x CVE security vulnerabili... x NVD - Vulnerability Deta... x CVE - Common Vulnerabi... x NVD - CVE-2011-1473 x CVE-2011-1473: \*\* DISPU x +

cveform.mitre.org

Apps İş Gücü Girişi Jira İş Gücü Confluence SGE Log in to bya USVN SGE UCROWD SGE Sanal Siber Gü... SiberLab3 SGE OpenStack Ge... SGE Udemey Google Slaytlar YÖKDİL Sınavı Reading list

**CVE**

Optional

Has vendor confirmed or acknowledged the vulnerability?  Yes  No

Attack type

Impact  Code Execution  Information Disclosure  
 Denial of Service  Other  
 Escalation of Privileges

Affected component(s)  
Please separate with commas. Examples of affected components: affected source code file, affected function, affected executable, etc.

Attack vector(s)  
What are the methods of exploitation? Example: to exploit vulnerability, someone must open a crafted JPEG file.

Suggested description of the vulnerability for use in the CVE

CVE - Common Vulnerabilities and Exposures (CVE) - Chromium

Google Çeviri x CVE security vulnerabili... x NVD - Vulnerability Deta... x CVE - Common Vulnerabi... x NVD - CVE-2011-1473 x CVE-2011-1473: \*\* DISPU x +

cveform.mitre.org

Apps İş Gücü Girişi Jira İş Gücü Confluence SGE Log in to bya USVN SGE UCROWD SGE Sanal Siber Gü... SiberLab3 SGE OpenStack Ge... SGE Udemey Google Slaytlar YÖKDİL Sınavı Reading list

**CVE**

Reference(s)  
Please include one reference/URL per line including protocol and domain name, e.g.,  
www.link.com  
https://link.org

Additional information  
Please provide any additional information you want to share with us here.

By clicking the submit button, you are agreeing to the CVE Terms of Use.

Enter Security Code

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

[https://cve.mitre.org/about/cve\\_and\\_nvd\\_relationship.html](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/>