

[← Listeye Dön](#)

## TR-24-1859 (django CMS Ürünü Güvenlik Bildirimi)

### Genel Bilgi

Açık kaynak bir proje olan "django CMS" ürünü için bildirilmiştir.

### Etki

Mevcut güvenlik açıklığı nedeniyle siber saldırılar gerçekleştirilerek kullanıcı bilgileri çalınabilir ve sistemler zarar görebilir. Zafiyet kodu şöyledir:

CVE-2024-11319

### Çözüm

Ulusal Siber Olaylara Müdahale Merkezi (USOM) kullanıcı ve sistem yöneticilerine dokümanı gözden geçirmelerini ve ürünü en az 4.1.4 versiyonuna yükseltmelerini tavsiye etmektedir.

### Kaynaklar

<https://iltosec.com/blog/post/django-cms-413-stored-xss-vulnerability-exploiting-the-page-title-field/>

<https://www.django-cms.org/en/blog/2024/11/13/django-cms-security-update/>

<https://github.com/django-cms/django-cms/commit/241d1cbe47a68f5d271ce4d27ad5e32e2c360ec3>

<https://www.cve.org/CVERecord?id=CVE-2024-11319>

#### Hızlı Menü

[İhbar Formu](#)[CVE Başvuru Formu](#)[Zararlı Bağlantılar](#)[Güvenlik Bildirimleri](#)

Yasal uyarılara ilişkin ayrıntılı bilgilere erişmek için lütfen [buraya tıklayınız](#).

[Tamam](#)



TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI  
SİBER GÜVENLİK BAŞKANLIĞI



TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI  
SİBER GÜVENLİK BAŞKANLIĞI

Türkiye Cumhuriyeti Siber Güvenlik Başkanlığı, Türkiye'nin siber güvenliğini sağlamak, mevcut ve muhtemel tehditleri tespit ederek bertaraf etmek ve geleceği temin etmek amacıyla Cumhurbaşkanlığına bağlı yerel bir kurumdur.

## Kurumsal

Başkanlık Hakkında

Teşkilat Şeması

Mevzuat

## Faaliyet Alanları

Siber Güvenlik

Dijital Devlet

Kamu Yapay Zekâ

Ekosistem Geliştirme

## Hızlı Bağlantılar

Sıkça Sorulan Sorular

Yasal Uyarılar



### Hızlı Menü

[İhbar Formu](#)

[CVE Başvuru Formu](#)

[Zararlı Bağlantılar](#)

[Güvenlik Bildirimleri](#)

Yasal uyarılara ilişkin ayrıntılı bilgilere erişmek için lütfen [buraya tıklayınız](#).



### Hızlı Menü

İhbar Formu

CVE Başvuru Formu

Zararlı Bağlantılar

Güvenlik Bildirimleri

Yasal uyarılara ilişkin ayrıntılı bilgilere erişmek için lütfen [buraya tıklayınız](#).