**Active Mixed Content over HTTPS (HTTPS Üzerinden Etkin Karmaşık İçerik)**



**MEDIUM**

**Özet**

Invicti, bir HTTPS sayfasında HTTP üzerinden etkin bir içeriğin yüklendiğini tespit etti.

**Etki**

Aktif İçerik, sayfanızın bağlamında çalışabilen ve ayrıca tüm sayfayı değiştirebilen bir kaynaktır. HTTPS sayfası, normal, açık metin HTTP aracılığıyla alınan komut dosyaları veya stil sayfaları gibi etkin içerik içeriyorsa, bağlantı yalnızca kısmen şifrelenir. Şifrelenmemiş içeriğe koklayıcılar erişebilir. Ortadaki adam saldırganı, HTTP içeriği talebini engelleyebilir ve ayrıca kötü niyetli kodlar eklemek için yanıtı yeniden yazabilir. Kötü amaçlı etkin içerik, kullanıcının kimlik bilgilerini çalabilir, kullanıcı hakkında hassas veriler elde edebilir veya kullanıcının sistemine kötü amaçlı yazılım yüklemeye çalışabilir (örneğin, tarayıcıdaki veya eklentilerindeki güvenlik açıklarından yararlanarak) ve bu nedenle bağlantı artık korunmaz.

**Düzeltme**

Karışık içerik sorunlarına karşı savunmak için iki teknoloji vardır:

* HTTP Strict Transport Security (HSTS), kullanıcı hataları (80 numaralı bağlantı noktasından web sitenize erişme girişimi) ve uygulama hataları (geliştiricileriniz güvenli bir sayfaya güvenli olmayan bir bağlantı yerleştirir) karşısında bile güvenli kaynak alımını zorlayan bir mekanizmadır.
* İçerik Güvenliği Politikası (CSP), üçüncü taraf web sitelerinden güvenli olmayan kaynak alımını engellemek için kullanılabilir.
* Son olarak, kullanıcının hangi protokole bağlı olduğuna bağlı olarak, kullanıcının tarayıcısının HTTP veya HTTPS'yi uygun şekilde otomatik olarak seçmesini sağlamak için "protokol göreli URL'leri" kullanabilirsiniz. Örneğin:

Bir stil yüklemek için protokole göre bir URL şöyle görünür:

<link rel="stylesheet" href="//example.com/style.css"/>

Komut dosyaları için:

<script type="text/javascript" src="//example.com/code.js"></script>

Tarayıcı, hangisi uygunsa, URL'nin başına otomatik olarak;

"http:" veya "https:" ekler.

Mertcan Taşkıran - 195541303