1.1.1 Eski Web Tarayıcılar için Clickjacking Önlemi Eksikliği (Potential Clickjacking on Legacy Browsers) (CWE-693)

Açıklık Önem Derecesi: Düşük

Açıklığın Etkisi: Kullanıcı Fark etmeden Kullanıcıya İşlem Yaptırma

Açıklığın Barındıran Dosyalar/Satırlar:

Proje Dosyası/Dosya Adı	Satır Numarası

Açıklığın Açıklaması:

Bir web sayfada kullanıcının fare tıkının çalınmasına clickjacking saldırısı adı verilir. Bu saldırıda web sayfa görünmez olarak <iframe>'lenir ve sahte/korsan bir web sayfanın üzerine bindirilir veya web sayfa görünmez olarak <frame>lenir ve açıklıklı web sayfanın üzerine bindirilir. Kullanıcı ilgili sayfada tık işlemi yaptığında (örn; bir linke veya butona tıkladığında) kullanıcının fare tıkı aslında görünmez olan açıklıklı web sayfasında çalışır. Bu durum kullanıcının açıklı web sayfada beklemediği, arzu etmediği eylemleri gerçekleştirmesine yol açabilir. Örneğin kullanıcı ayarlarını değiştirme, kullanıcı kayıtlarını silme, kullanıcı webcam'ini aktifleştirme (enable etme),… gibi.

Bu açıklık saldırganın özel hazırlanmış üst katman oluşturmasına izin verir. Açıklığın temel sebebi ise web uygulamanın web sayfalarının bir başka web uygulamasına veya aynı web uygulamaya frame olarak yüklenebilir olmasındandır.

Web uygulama bir web sayfasının frame içerisinde yüklenebilmesini önleyen uygun bir frame-busting script önlemi uygulamalıdır. Modern web tarayıcılar söz konusu iken uygulamalar bu açıklığı uygun bir Content-Security-Policy veya X-Frame-Options yanıt başlıkları ile kapatabilirler. Ancak birçok eski web tarayıcıda bu yanıt başlıkları (bu özellik) desteklenmemektedir. Bu nedenle bu açıklığı Javascript ile giderecek daha manuel bir yaklaşıma ihtiyaç vardır. Sonuç olarak eski web tarayıcılarda clickjacking saldırılarını önlemek için frame-busting script'i kullanılmalıdır.

Frame-Busting önlemi barındırmayan Clickjacking açıklıklı web sayfaları "Eski Web Tarayıcılar İçin Clickjacking Önlemi Eksikliği" (CWE-693) açıklığı şeklinde işaretlenirler. Bu açıklığı örneklemek maksadıyla "Eski Web Tarayıcılar İçin Clickjacking Önlemi Eksikliği" açıklığı barındıran bir web sayfası örnek olarak verilmiştir.

Açıklıklı X Web Sayfası:

```
<html>
    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Piyasada bu açıklığı kapamaya dönük çok çeşitli Frame-busting önerileri vardır ve çoğu güvensizdir. Bu web sayfasına güvensiz (güvenliği atlatılabilir) frame-busting önlem kodu konulduğu hale şu şekilde bir örnek verilebilir.

Güvensiz (Güvenliği Atlatılabilir) Frame-Busting Önlemli X Web Sayfası:

```
<html>
    <head>
        <script>
            if ( window.self.location != window.top.location ) {
                window.top.location = window.self.location;
            }
        </script>
    </head>

    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Bu önlem frame'lenen sayfa için frame html etiketine konulacak sandbox attribute'u (özelliği) ile atlatılabilir (bypass'lanabilir) ve clickjacking saldırısı frame-busting önlemine rağmen başarılı olabilir. Bu nedenle güvenli Frame-Busting kodu kullanılmalıdır. Web sayfanın güvenli frame-busting önlemli hali şu şekilde olacaktır:

Güvenli Frame-Busting Önlemli X Web Sayfası:

```
<html>
    <head>
        <style> html {display : none; } </style>
        <script>
            if ( self === top ) {
                document.documentElement.style.display = 'block';
            }
            else {
                top.location = self.location;
            }
        </script>
    </head>

    <body>
        <button onclick="clicked();">
            Click here if you love ducks
        </button>
    </body>
</html>
```

Kurum web uygulamasında eski web tarayıcılar için clickjacking saldırılarına karşı önlem uygulanmadığı tespit edilmiştir. Bu durum Şekil XXX. ABCDEF'de gösterilmiştir.

::::::::BULGU::::::::::

Açıklığın Önlemi:

Önlemler için genel olarak takip edilmesi gereken adımlar şu şekildedir:

- Sunucu tarafta frame-ancestors direktifli CSP yanıt başlığı tanımlanmalıdır ve uygulanmalıdır. CSP yanıt başlığı tüm ilgili web sayfalarda yanıt paketinde gelmelidir.
- Eğer belirli web sayfaların bir frame'e yüklenmesi gerekliyse bu durumda ilgili URL'ler beyaz liste olarak tanımlanmalıdır.
- Alternatif olarak tüm yanıt paketlerinde X-Frame-Options yanıt başlığı kullanılabilir. Eğer belirli web sayfaların bir frame'e yüklenmesine izin vermek gerekiyorsa ilgili URL'ler beyaz liste olarak tanımlanmalıdır.
- Eski web tarayıcılar için Javascript ve CSS ile frame-busting önlemi uygulanmalıdır. Bu önlem ile eğer bir web sayfa frame'lenirse hiç gösterilmez ve frame'lenen sayfaya yönlendirme tetiklenir. Eğer yönlendirme başarısız olursa web sayfa gösterilmediğinden etkileşimli olmayacaktır ve clickjacking saldırısı başarısız olacaktır.

Önlemler için spesifik tavsiyeler şu şekildedir:

- İstemcide frame-busting atlatma saldırılarına karşı zafiyetli olmayan uygun bir frame-busting script'i kullanılmalıdır.
    - Frame-Busting kodu ilk olarak arayüzü (User Interface'i (UI'ı)) deaktif etmelidir. Öyle ki şayet frame-busting atlatılabiliyor olsa bile arayüz (User Interface (UI)) tıklanamazdır. Bu <body> veya <html> etiketlerinin display özelliği (attribute) değerini "none" şeklinde ayarlayarak yapılabilir. Bu <body> veya <html> için display="none" işlemi yapılmalıdır, çünkü eğer bir frame (parent'ı) ana sayfayı yönlendirmeye teşebbüs ettiğinde ve parent (ana sayfa) olmaya çalıştığında zararlı parent (ana sayfa) halen çeşitli teknikler ile yönlendirmeyi önleyebilir ve bu durumda clickjacking meydana gelebilir. Fakat display="none" ile bunun önüne geçilir.
    - Frame-Busting kodu daha sonra self === top kıyaslaması yaparak web sayfada frame'leme olup olmadığını saptamalıdır. Eğer kıyaslama sonucu true ise bu durumda arayüz (User Interface (UI)) aktif edilebilir. Eğer kıyaslama sonucu false ise top.location özelliği (attribute'u) self.location (attribute) değerini alarak frame'i kullanan sayfadan uzak bir yere (frame'lenen sayfaya) yönlendirme teşebbüsü uygulanmalıdır.

Önerilerden hareketle güvenli Frame-Busting önlemi şu şekildedir:

```
<html>
    <head>
        <style> html {display : none; } </style>
        <script>
            if ( self === top ) {
                document.documentElement.style.display = 'block';
            }
            else {
                top.location = self.location;
            }
        </script>
    </head>
    ...
    ...
</html>
```

Referanslar:

1. https://cwe.mitre.org/data/definitions/693.html