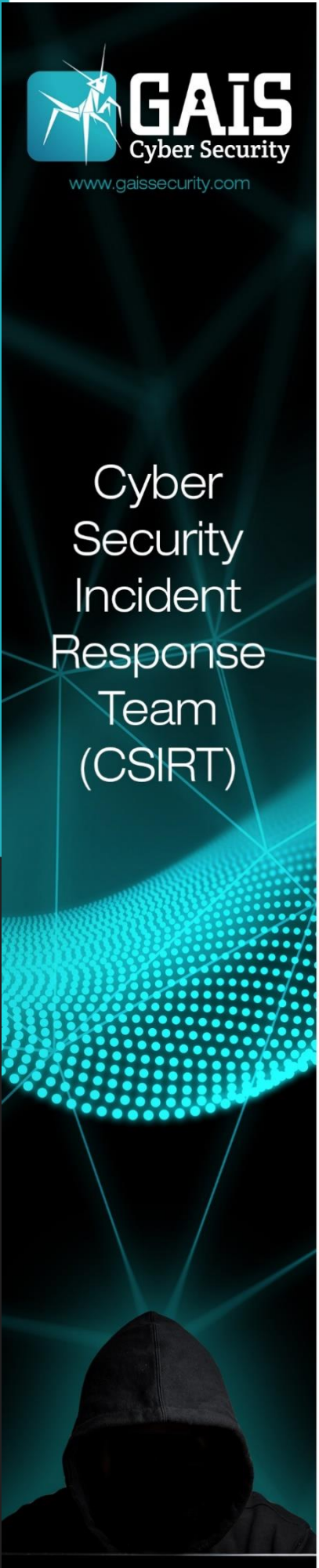
GAIS Cyber Security

www.gaissecurity.com

Cyber Security Incident Response Team (CSIRT)



@gaissecurity

Siri Uygulaması Güvenlik Açığı Raporu

CVE-2017-13805

28.01.2018

Hazırlayan:

Yiğit Can Yılmaz

[Security Researcher]

Adres : Saray Mh. Doktor Adnan Büyükdeniz Cd. No:4
Akkom Office Park 2.Blok. 10/21 Ümraniye / İstanbul - Turkey
Web : www.gaissecurity.com Tel : 0216 250 32 82

ÖZET

Apple’ın kişisel asistanı Siri kullanıcı tarafından kilit ekranında erişimine engellenmiş bildirimleri ve içeriklerini kilit ekranında kullanıcı izni olmadan söyleyebilir.

Apple'ın sanal asistan uygulaması olan ve iOS işletim sistemine sahip cihazlarında kullanılabilen Siri isimli uygulama sizin sorularınıza yanıt veriyor ve telefonunuzun çeşitli uygulamalarını sesli komut ile kullanabilmenize imkan veriyor. Ayrıca Siri sizin yapmış olduğunuz ayarları da okuyan Siri , güvenlik amacıyla da bazı durumlarda ne yapması gerektiğini öğreniyor. Örneğin Siri, eğer cihazınızda bir Parola & Touch ID koruması etkin ise parolanızı ya da parmak izinizi cihaza girmeden birçok işlemi gerçekleştirmiyor.

Fakat Siri, Ayarlar > Parola & Touch ID bölümünde denetlemesi gereken “Son Bildirimler” seçeneğinin etkin olup olmadığını denetlemiyor. Bu sayede iOS cihazına kullanıcıdan izinsiz erişen bir kişi kullanıcı izni olmadan kilit ekranında bildirimleri ve içeriklerine erişebiliyor.

Güvenlik Açığını Oluşturma Adımları

- Siri etkin değil ise Ayarlar üzerinden veya Ev tuşuna basarak Siri'yi etkinleştirin.
- Ayarlar'a gidin.
- Touch ID & Parola bölümüne girin.
- "Kilitliyken Erişime İzin Ver" bölümünden "Son Bildirimler" seçeneğini kapatın.
- Kendi cihazınıza farklı bir cihaz ve herhangi bir uygulamadan mesaj göndererek bildirim gelmesini sağlayın.
- iCihazı(iPad,iPod,iPhone) kilitleyin.
- Ev tuşuna basarak Siri'yi açın.
- "Bildirimler" deyin.
- Bir süre bekleyin.

Siri size hangi uygulamadan bildirim geldiğini ve bildirim içeriklerini sesli olarak okuyacaktır.

Güvenlik Açığını Apple firmasına Bildirim Süreci

Kullanıcı tarafından bildirimlerin kilit ekranında erişimi engellenmesine rağmen Siri'nin bildirim sayılarını ve bildirimlerin içeriklerinin okunabildiği tespit edilmiştir.

- 01.08.2017 tarihinde güvenlik açığı Apple Ürün Güvenliği Ekibine bildirildi.
- 01.08.2017 Apple tarafından takip numarası verildi.
- 13.09.2017 Apple Ürün Güvenliği raporu bir güvenlik sorunu olarak kabul etti ve sorunu çözmek için çalışmalar başladı.
- 31.10.2017 Apple iOS 11.1 güncellemesini yayınladı ve mail listesine eklendi. (https://lists.apple.com/archives/security-announce/2017/Oct/msg00000.html)
- 01.11.2017 Apple Ürün Güvenliği ekibine güvenlik sayfasına zafiyeti tespit eden Yiğit Can YILMAZ adı eklendi.

Siri

İlgili Ürünler: Iphone 5S ve sonraki modeller, iPad air ve sonraki modeller, iPod touch 6. Nesil

Etki: iOS aygıtına fiziksel olarak erişilebilen bir kişi, kilitli ekranda gösterilmeyecek şekilde ayarlanan içerikl bildirimlerini Siri' yi kullanarak okuyabilir.

Açıklama: siri izinlerinde bir sorun vardı. İzin denetimini iyileştirilerek bu sorun giderildi.

CVE ID: CVE-2017-13805

iOS 11.1 güncelleştirmesinin güvenlik içeriğine şuradan erişebilirsiniz:
https://support.apple.com/tr-tr/HT208222