ZOOM KRİTİK ZAFİYET RAPORU

Hassas Veri İfşası ve Güvensiz Doğrudan Nesne Erişimi

www.gaissecurity.com

@gaissecurity

COVID-19 pandemisi ile birlikte dünyada toplumsal yaşam standartları ve alışkanlıklar hızla değişirken, kurumsal ve özel sektörlerde farklı ihtiyaç alanları ortaya çıkmıştır. Bu ihtiyaçların başında ise kurumsal süreçlerin olağanüstü bu durumun karşısında firmaları hızlı reaksiyon alması ve iş süreçlerini normalleştirmek amacıyla video konferans uygulamalarına yönlendirmiştir.

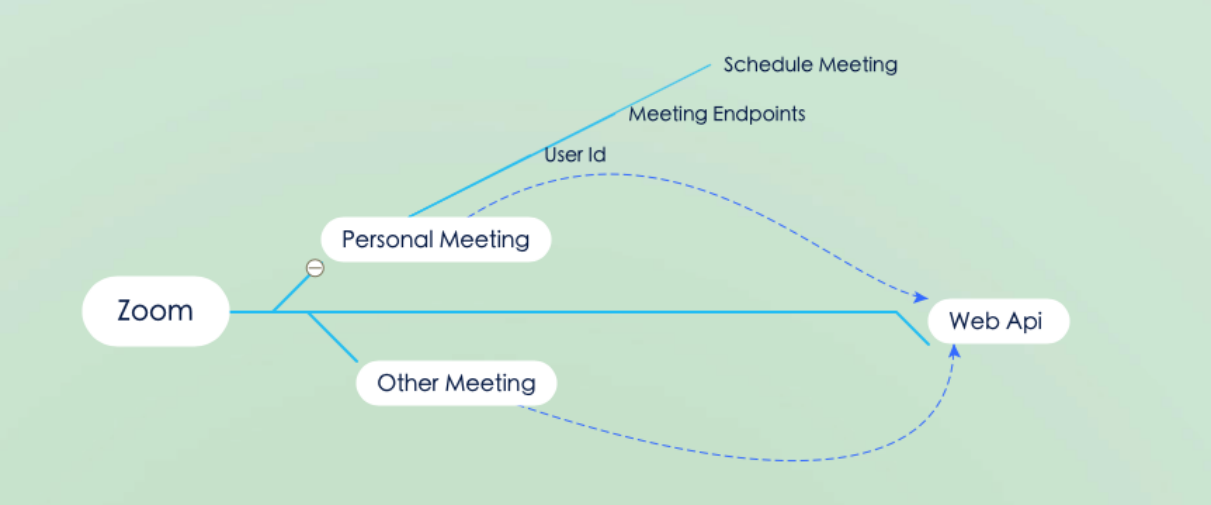
Gais CERT ve Gais Cyber Intelligence tarafından 500.000'in üzerinde bireysel ve kurumsal Zoom hesabının Dark Web ve illegal forumlarda sızdırıldığı tespit edilmiştir. Sızdırılan hesapların bir kısmı açık halde sunulurken, bir kısmı da ücret karşılığında satıldığı görülmüştür.

Zoom uygulaması, firmaların ihtiyaçlarını karşılaması adına birçok sektörde rağbet gören yaygın bir video konferans uygulaması olduğu ve bu çözümlerin kullanımı olası güvenlik ihlallerinde ne gibi riskler oluşturacağını ortaya koyma adına, Gais Security tarafından analiz edilmiştir. Yapılan analiz sonucu elde edilen güvenlik açığı Zoom yetkilileri ile paylaşılmış ve $1000 ödül verilmiştir.

hackerone

Zoom rewarded you with a bounty of **$1,000** for Sensitive Data Exposure & Insecure Direct Object Reference . If you're as excited as we are, go ahead and tweet about it!
Thank you for your report!
What's next?
Before we can begin the payment process, United States tax law requires that we collect some information from you. Please click the link below to request the right tax form. You'll only need to do this once.
Sign tax form

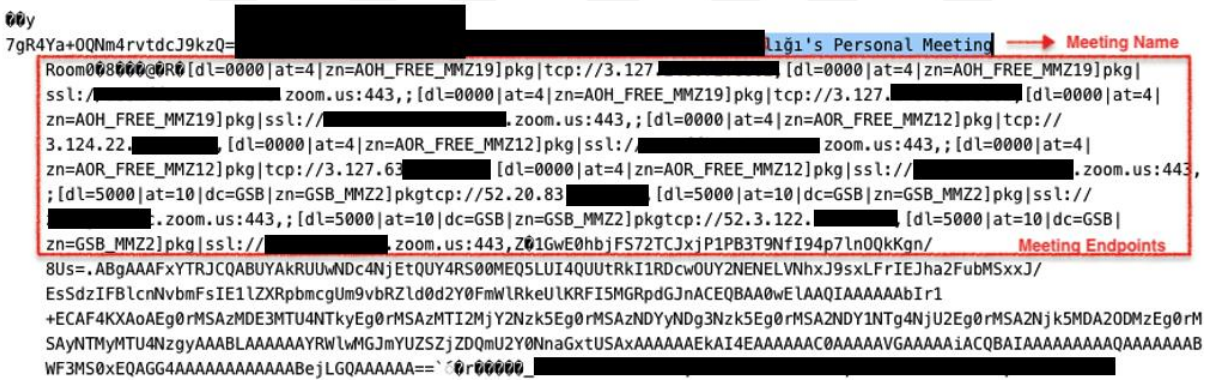
Gais Security tarafından yapılan analizlerde tespit edilen güvenlik açığına ilişkin tüm detaylar Zoom yetkilileri ile paylaşılmış ve ilgili güvenlik açığı hızlıca kapatılmıştır. Fakat alınan önlemler daha önce oluşturulan toplantıların güvenliğini sağlamadığı için, son kullanıcı güvenliği düşünülerek ve riskin boyutlandırılması adına rapor paylaşılmıştır. Gais Security tarafından güvenlik açığına ait detayların Zoom firma yetkilileri ile paylaşılması yüz binlerce kullanıcının verilerinin sızmasını engellemiştir.



Zoom uygulamasının web servisinde fuzzing işlemleri uygulanarak tespit ettiğimiz bir dizinde "Personel Meeting" ve "Other Meeting" olarak adlandırdığımız kullanıcıların oluşturduğu veya random üretilen id numaralarına yönelik detaylı bilgilerin çekilebildiği tespit edilmiştir.

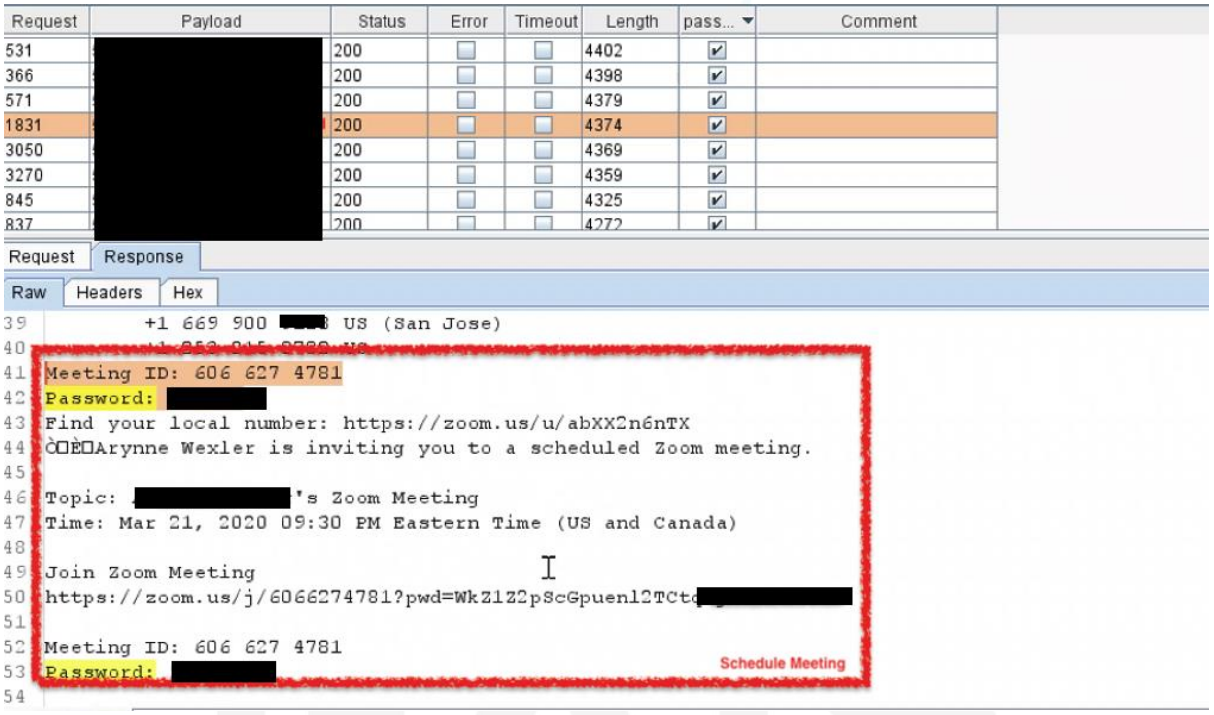
Other Meeting

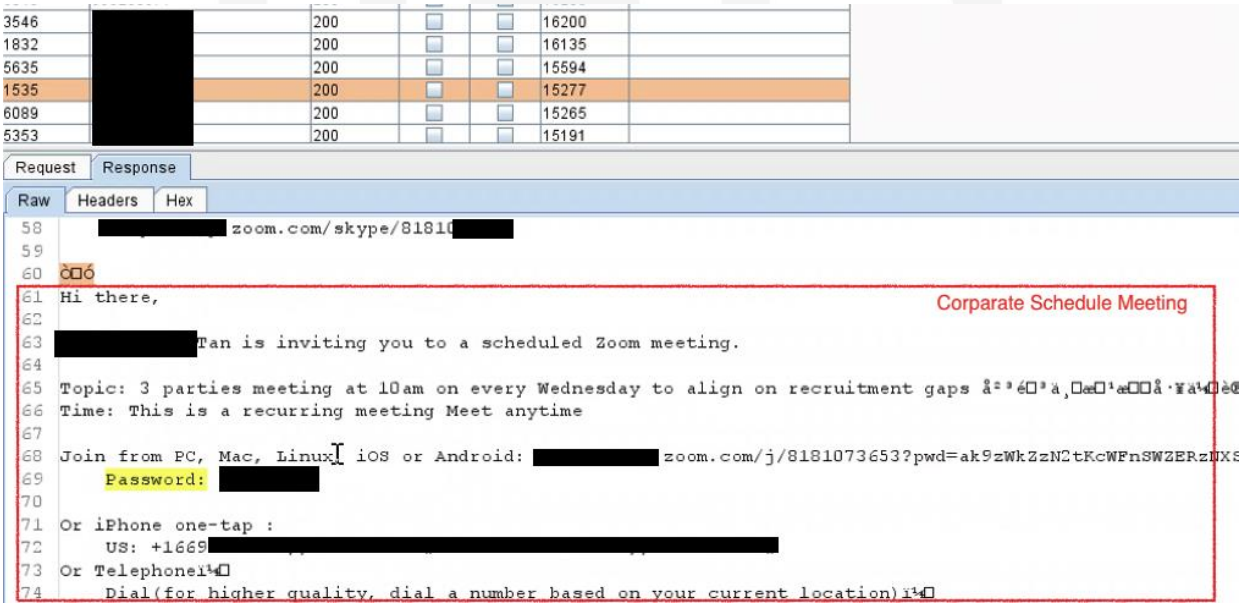
Bu kategoride yayında olan veya geçmiş toplantı odalarına ait konu kısımları, oluşturan kullanıcıya ait UserId numarası ve kullanıcının yerel veritabanında bulunan "meeting endpoint" bilgilerine erişildiği tespit edilmiştir.



Personal Meeting

Bu kategoride ise Zoom uygulamasının güvenlik mimarisini oluştururken zorunlu parola kullanımının bulunmamasından kaynaklı olarak hassas veri ifşasına neden olduğu gözlemlenmiştir. 9 ila 11 hane arasında random numaralar ile üretilen "Personal Meeting" numaralarının fuzz edilmesi sonucunda kullanıcıların "Schedule Meeting" olarak atandığı ileri tarihli toplantı kayıtlarına ait parolalarına erişildiği tespit edilmiştir. İlgili adreste toplantı id değerlerine yönelik yapılan kaba kuvvet saldırılarında yüz binlerce kişisel ve kurumsal hesaplara yönelik toplantı bilgilerine ve parola bilgilerine erişilmiştir.





İlgili zafiyetin bildirilmesi ile beraber alınan güvenlik önlemlerini şu şekilde listeleyebiliriz;

- Mayıs ayından sonra yeni bir kullanıcı oluşturulduğunda “Personal Meeting” id numarasına parola atanması.
- “Schedule Meeting” oluşturulurken zorunlu parola ataması yapılması.
- Toplantılara yeni katılan kullanıcıların moderatör tarafından onaylanarak video konferans sistemine dahil edilmesi.
- Web uygulaması üzerinde hassas bilgilerin maskeleme işlemlerine tabi tutulması.

Tespit edilen bu güvenlik zafiyeti ve alınan önlemler sonucunda Mayıs ayından önce açılan ve “Personal Meeting” adreslerine parola ataması gerçekleştirmeyen yüz binlerce kullanıcıyı etkilemeye devam ettiği Zoom yetkililerine raporlanmıştır.