Heartbleed

Barış Can

Nisan, 2014

Heart, ingilizce kalp anlamına gelen bir kelime; bleed ise kanama. İki kelimeyi birleştirdiğimizde, "kalp kanaması" çıkıyor ortaya, güzel de oluyor; zira ben internet dünyasının %70'ini etkileyecek bir zaafiyet keşfetsem, ben de aynı ismi koyardım. Zaafiyet, ilk olarak Codenomicon şirketinin Riku, Anti ve Matti isimli üç güvenlik uzmanı tarafından keşfedildi. Elbette ardından ilk iş olarak OpenSSL geliştiricilerine raporlandı analizler. Günlerdir zaafiyetle ilgili süregelen tartışmalar ve iddialar mevcut; en önemlisi is NSA, yani ABD Ulusal Güvenlik Ajansı'nın bu açığı yaklaşık iki yıldır biliyor olup, istihbaratvari durumlar için yararlanması. NSA twitter hesabından zaafiyetten haberdar olmadıklarını belirtmiş fakat akıllarda hâlâ soru işaretleri mevcut.

"Nereden bulmuşlar ki bu zaafiyeti?" diye soruyorsunuz, farkındayım.

Zaafiyet, OpenSSL kütüphanelerinde bulunan **"heartbeat"** isimli bir eklentiden kaynaklanıyor. Zaten ismi biraz da buradan geliyor.

Girişi biraz şenlendirdiğimize göre hadi biraz derinlere inelim.

OpenSSL, SSL/TLS protokol hizmeti sağlayan bir uygulama ve internet dünyasının büyük patronları dahil –yahoo, twitter,google– çoğu web sitesi uygulamayı kullanmakta. Pratikte; kötü amaçlı korsanımız, bu zaafiyete sahip sistemlerinin bilgilerine –kullanıcı adları, şifreler, sertifikalar, e-posta yazışmaları, vs. – erişebiliyor ve dahası, ele geçirebiliyor. Zaafiyet önemli, çünkü iz bırakmıyor; korsan işini sessizce hallediyor ve sistemden çıkışını gerçekleştiriyor. Zaafiyetin iz bırakmamasının sebebi OpenSSL loglarının şifreli bir biçimde kodlanmış olması. Teorik olarak, bu uygulama zaten "koruma" için kullanılıyor ve loglarının şifrelenmesi gayet normal; korunamadıkları ise, aşikâr. Mobil işletim sistemi olan Android de geçtiğimiz günlerde zaafiyetten payını aldı. Google'dan yapılan açıklamada Android 4.1.1 sürümünün açıktan etkilendiği bildirildi ve şu an android kullanıcılarının %34 gibi bir kısmı bu sürümü kullanmakta. Zaafiyet eklentiden kaynaklı, yani uygulamanın temelinden vazgeçmenizi gerektirecek bir durum söz konusu değil; zaten geçtiğimiz günlerde hakkında birçok "fix" yani, güvenlik güncellemesi de çoktan yayınlandı.

Gelelim nasıl korunabileceğimize;

Öncelikle, mobil işletim sistemi olan Android de geçtiğimiz günlerde zaafiyetten payını aldı. Google'dan yapılan açıklamada Android 4.1.1 sürümünün açıktan etkilendiği bildirildi ve şu an android kullanıcılarının %34 gibi bir kısmı 4.1.x sürümünü kullanmakta. Korunabilmenizin şu an için tek çözümü güncelleme paketiniz var ise derhâl kurmak. Bunun dışında, üçüncü parti firmaların Google Play Store'de yayınladıkları uygulamaları –güvenli olduklarını düşünüyorsanız– kullanabilirsiniz.

OpenSSL 'in aşağıdaki sürümlerinden birini kullanıyorsanız, güvenlik güncellemesini yapmanızda fayda var;

```
1 OpenSSL 1.0.1e-fips
2 OpenSSL 1.0.1 1.0.1f
```

Bir de varsayılan olarak, yani kurulduğunda OpenSSL ile gelen işletim sistemleri var, sürümlerine göre bunlar da zaafiyet içeriyor olabilirler;

- Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
- Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
- CentOS 6.5, OpenSSL 1.0.1e-15
- Fedora 18, OpenSSL 1.0.1e-4
- OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) and 5.4 (OpenSSL 1.0.1c 10 May 2012)
- FreeBSD 10.0 – OpenSSL 1.0.1e 11 Feb 2013
- NetBSD 5.0.2 (OpenSSL 1.0.1e)
- OpenSUSE 12.2 (OpenSSL 1.0.1c)

OpenSSL sürümünüzü "openssl version" komutuyla komut satırından öğrenebilirsiniz.

Mevcut işletim sisteminize dair bir güncelleme paketiniz yok ise, önerilen tek çözüm yolu **"-DOPENSSL_NO_HEARTBEATS"** parametresi ile OpenSSL uygulamanızı yeniden derlemek.

Zaafiyet çok ciddi tehlikelere yol açabilecek ve bunu siz farketmeden yapacak türde. Bu yüzden dikkatli olmanızı öne-rerek bitiriyorum.

Bir sonraki yazımda görüşmek üzere.