Android Stagefright Vulnerability

written by Mert SARICA | 1 September 2015

As a person who is really interested in social networks, the trend of creating business-oriented Whatsapp groups on LinkedIn takes my attention. In this trend, someone is creates a Whatsapp group and announces it on LinkedIn. Then other people drop a comment below with their phone number, state that they want to join that group. Afterwards the creator of the group adds them to the group one by one.


19:07
18%
2 g
İnsan Kaynakları Yöneticisi
İnsan Kaynakları meslektaşlarımızdan oluşan Whatsapp grubumuza katılmak isterseniz, iletişim numaranızı benimle paylaşabilirsiniz. İyi çalışmalar.
18 Beğenme
47 Yorum
+13
Eski yorumları görüntüle ...
2 g
İnsan Kaynakları Yöneticisi
Şuan ekibimiz 46 kişiden oluşuyor. Meslektaşlarımıza faydalı olacağını düşünüyorum.
2 g
İnsan Kaynakları Yöneticisi
İnsan Kaynakları çalışanlarının dışında gelen talepler için malasef olumlu geri dönüş yapamıyorum.
Yorum Yap...

19% 19:05

1 g

Human Resources Manager -

Bey Merhaba, bende gruba katılmak isterim.

1 g

SUPERVISOR /

Merhaba 0538

1 g

İnsan Kaynakları Sorumlusu -

Merhaba 0541

1 g

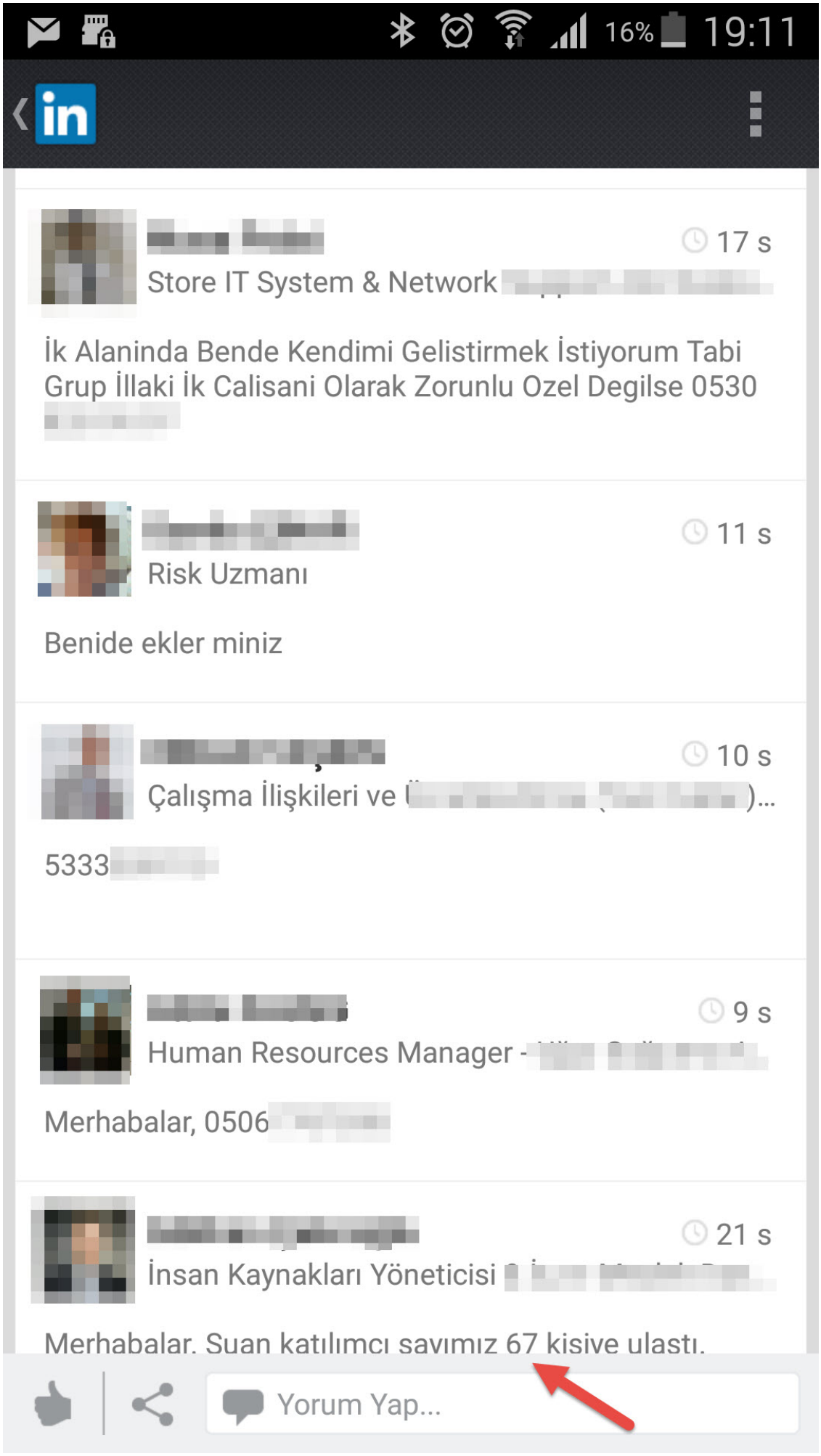
Social Media Manager at

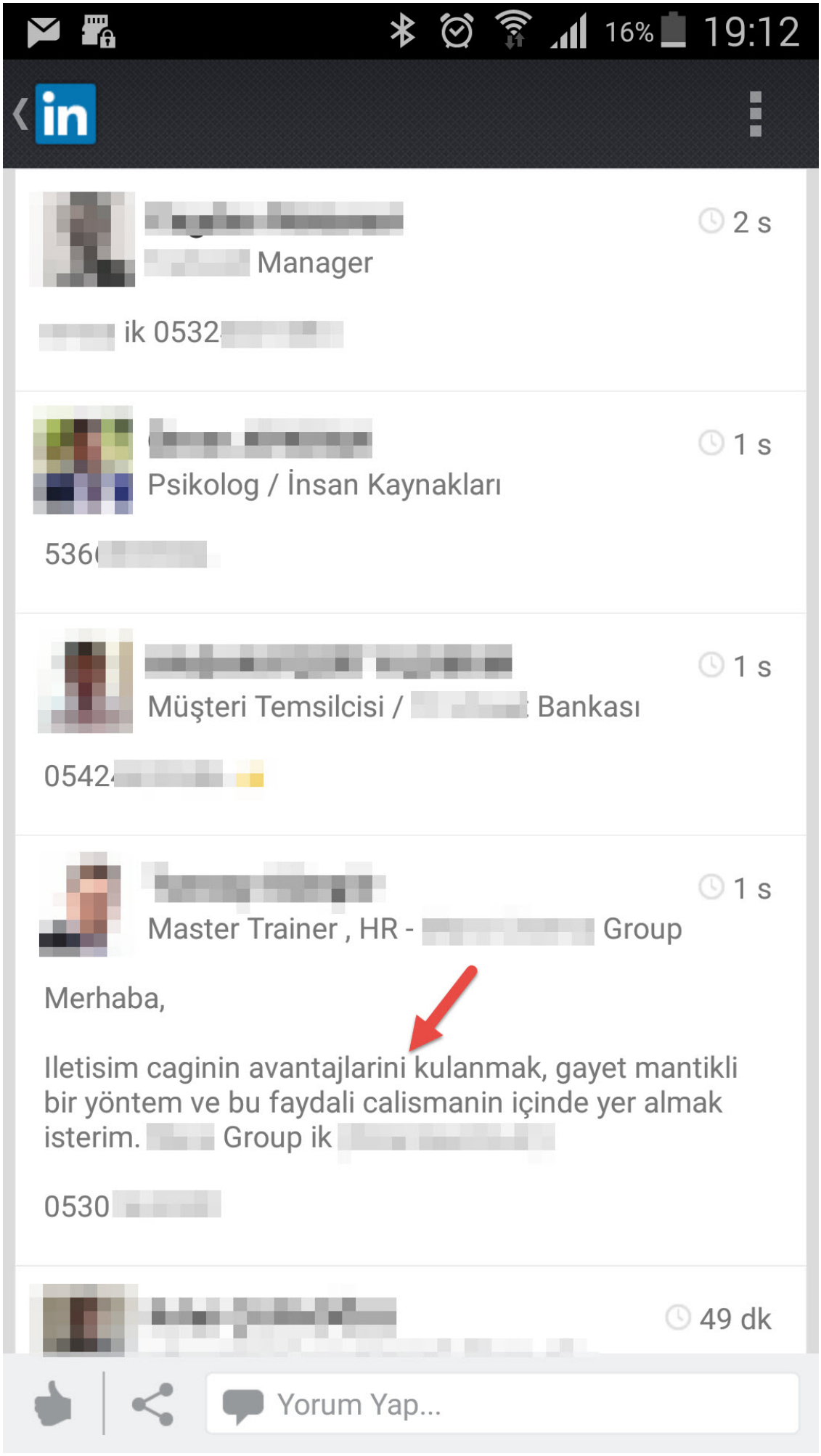
+90536

1 g

GRUBA KATILMAK İSTERİM 0 535

Yorum Yap...


16% 19:11
17 s
Store IT System & Network
İk Alaninda Bende Kendimi Gelistirmek İstiyorum Tabi Grup İllaki İk Calisani Olarak Zorunlu Ozel Degilse 0530
11 s
Risk Uzmanı
Benide ekler miniz
10 s
Çalışma İlişkileri ve
5333
9 s
Human Resources Manager -
Merhabalar, 0506
21 s
İnsan Kaynakları Yöneticisi
Merhabalar. Suan katılımcı sayımız 67 kisiye ulastı.
Yorum Yap...


16% 19:12
2 s
Manager
ik 0532
1 s
Psikolog / İnsan Kaynakları
536
1 s
Müşteri Temsilcisi / Bankası
0542
1 s
Master Trainer , HR - Group
Merhaba,
Iletisim caginin avantajlarini kulanmak, gayet mantikli bir yöntem ve bu faydali calismanin içinde yer almak isterim. Group ik
0530
49 dk
Yorum Yap...

In case you ask “What is the problem with that?” First of all; LinkedIn is a business-oriented social network and on there, you share various of information about your company and your position in that company, about your job and your workplace. We know that people with bad intentions about hacking a firm and intelligence agencies, target employees. Recent example to this would be; the documents leaked by Edward Snowden, we learned that U.S.A intelligence agency NSA and British intelligence service GCHQ hacked the emails and Facebook accounts of Gemalto’s employees in 2010, which is a global sim card manufacturer firm, to steal the sim card encryption keys. With this data, we can’t even imagine what they are doing in this century. Apart from intelligence agencies, we see that people with bad intensions target smart phones and also they target even smart watches.

In the past, the worst thing that can happen to you when you share your number on internet and/or any other platform would be some psycho disturbing you by calling you in the middle of the night and maybe waking you up. But in this era, the worst thing that can happen is very different (On my Evil Pi article I simulated how to abuse the Android phones that contains vulnerability). That psycho can turn into a hacker and those people, now, are able to steal all off your personal information.

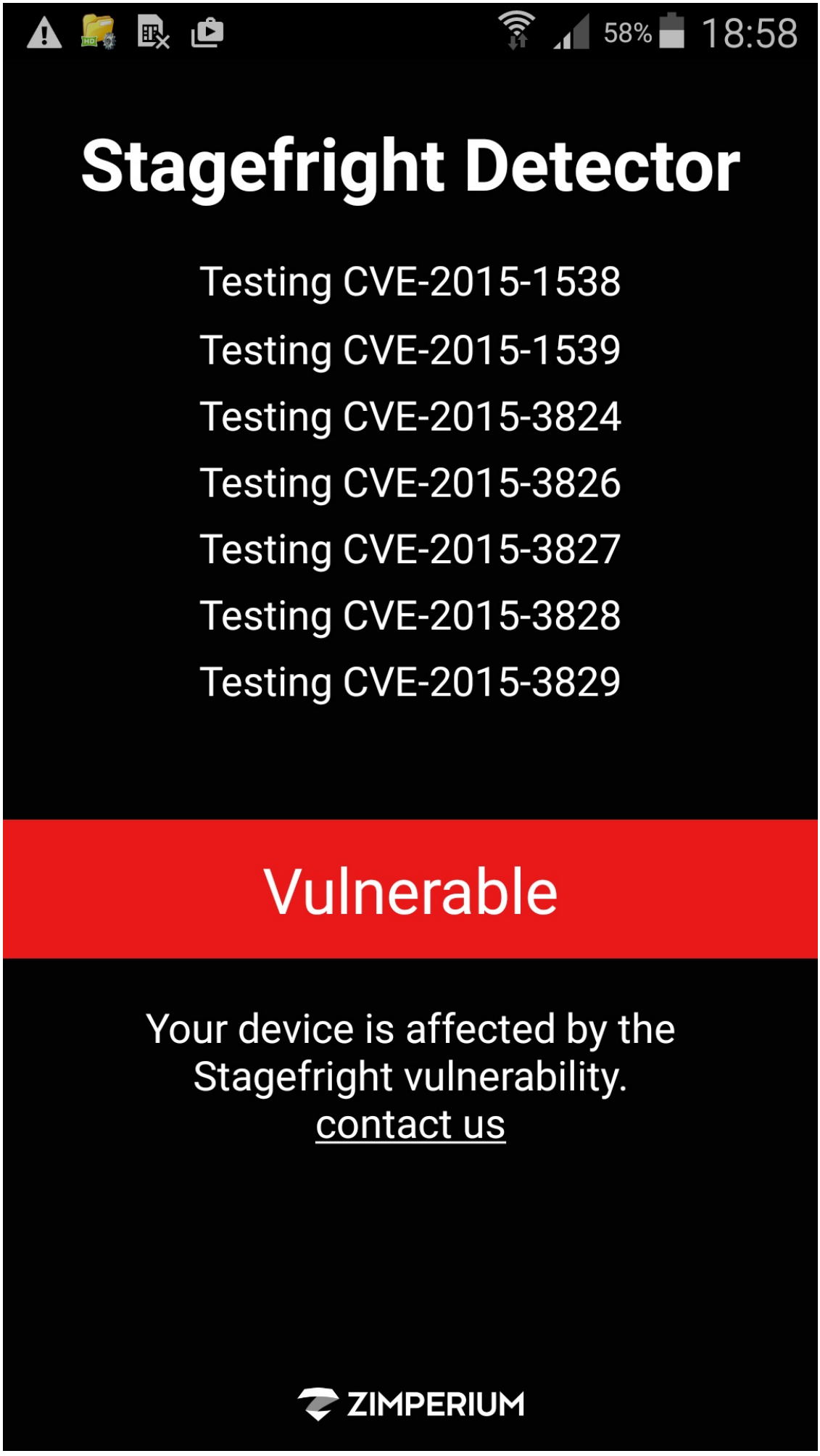
On Black Hat information security conference that took place on August 5th of 2015, details of a vulnerability that affects more than 950 million android devices has been shown by Joshua Drake (@jduck). To exploit this vulnerability, (to hack phones/tablets) knowing target’s phone number and sending a MMS with the exploit code or sending a link of a video in mp4 format is enough.

Even though Google instantly publishes the patches for Android OS, to download it to your phone it is required to wait for manufacturer firm (like Samsung) to make that patch downloadable to its phones. So although Google make patches after one dat the vulnerability is found, it is also mandatory for manufacturers to act really fast.

With the research of a firm named Exodus, it has been seen that Google couldn’t actually remove the vulnerability with that patch. It seems that

even on best case scenario we are not going to be able to install this patch before September.

Does that mean ‘we are going to sit there and do nothing?’ No. First of all; we can determine whether we are affected by this vulnerability or not with StageFright Detector tool.


58% 18:58
Stagefright Detector
Testing CVE-2015-1538
Testing CVE-2015-1539
Testing CVE-2015-3824
Testing CVE-2015-3826
Testing CVE-2015-3827
Testing CVE-2015-3828
Testing CVE-2015-3829
Vulnerable
Your device is affected by the Stagefright vulnerability.
contact us
ZIMPERIUM

Secondly; MMS is not the only attacking vector but it is the easiest one to exploit. So, to prevent the attacks coming from this vector, you can disable automatically retrieve an MMS option on your Android OS (Even if you disable it, when you manually receive those MMS's, don't forget that your device can still get hacked).

You can follow the steps below to prevent your device retrieving the MMS automatically.

For Android; Settings -> Messages -> Multimedia Messages (MMS) -> Auto Retrieve
For Google Hangouts; Hangouts -> Settings -> SMS -> Auto Retrieve MMS

If you are a Samsung user, you can also install the MMS Control application that is being launched by Samsung itself.

These steps shown above is not going to cover the vulnerability like a patch and Google says that it is not likely that this vulnerability can be abused to hack many phones because of the ASLR (address space layout randomization) security measure that came with in Android 4.0 "Ice Cream Sandwich". However it is always good to be careful until the patch comes out.

Finally, the fact that the cell phone numbers is enough to exploit the vulnerabilities of smartphones, can lead hackers to target the employees to be able hack the firm. For this reason, it is a good thing to be cautious even while sharing the phone numbers.

Hope to see you on the next article. I wish secure days to everyone.

Update: On 09.09.2015, exploit code for CVE-2015-1538 vulnerability has been published.

Original Article: Android Stagefright Zafiyeti
Translated to English by: Hüseyin Fatih Akar | Twitter: @thehakar)