Dear **< REDACTED >**

Firstly, thank you very much for alerting us to this blog re celebrite below. I agree with both yourself and **< REDACTED >** that it make sense to try and find out more information from Police Scotland about this. To that end I have included the portfolio lead for cyber kiosks **< REDACTED >** office in this email (in addition to **< REDACTED >** as the IAG Police Scotland representative).
Happy to discuss further in due course but have to go to another meeting now.
Thanks
Liz

Dr Liz Aston
Director,Scottish Institute for Policing Research

Associate Professor of Criminology
Edinburgh Napier University
School of Applied Sciences
< REDACTED >

From: **< REDACTED >**
Sent: 22 April 2021 07:39
To: **< REDACTED > < REDACTED >**
Cc: Aston, Liz; **< REDACTED > < REDACTED > < REDACTED >**
< REDACTED > < REDACTED > < REDACTED > < REDACTED > < REDACTED >
< REDACTED > < REDACTED > < REDACTED > < REDACTED > < REDACTED >
< REDACTED > Hicks, Clare;
Subject: RE: Urgent: exploitable vulnerability in Cellebrite / cyber kiosk systems

Hi **< REDACTED >**,

In terms of the IAG, it would be my recommendation that the group does not comment on this and, if you continue to be pressed, suggest that you refer the journalist to Police Scotland themselves at this stage. **< REDACTED >** - would appreciate if you could provide comment on this proposed approach and, if possible, your views on the veracity of the content of the blog.

From a Scottish Government perspective, I will forward on your email to my communications colleagues for information, should we be approached.

Thanks

< REDACTED >
-----Original Message-----
From: **< REDACTED >**
Sent: 21 April 2021 19:56
To: **< REDACTED >**
Cc: Aston, Liz; **< REDACTED > < REDACTED >**
< REDACTED > < REDACTED > < REDACTED > < REDACTED >

< REDACTED > < REDACTED > < REDACTED > < REDACTED > < REDACTED >
< REDACTED > < REDACTED > < REDACTED >
Subject: Urgent: exploitable vulnerability in Cellebrite / cyber kiosk systems
Importance: High

Good evening **< REDACTED >**,

Apologies for contacting you out of hours.

This evening, news has broken of a technical vulnerability in the Cellebrite software which is used in the cyber kiosks system used by Police Scotland:

https://signal.org/blog/cellebrite-vulnerabilities/

We have not been able to commission our own technical analysis after hours, so based on that blog post alone, we do not know if the vulnerability can be easily patched, or if it is, as the article suggests, a cascade of related issues. If it is the latter, and the systems can be easily tampered with, it would cast procedural doubt upon any evidence gathered using through the kiosks, and possibly challenge any convictions.

They have taken the unusual decision to publish this post rather than contact Cellebrite through a responsible disclosure programme, and have also hinted in the blog post that they are working on a Trojan horse against it, which makes this issue somewhat urgent.

I have already been contacted by a journalist seeking comment from us **< REDACTED >** on the issue. Given our participation on the IAG, we do not want to make a comment based on a single blog post before Police Scotland has had a chance to investigate the vulnerability. Can I refer them to you?

Regards,
< REDACTED >

Annex B

From: **< REDACTED >**
Sent: 22 April 2021 15:43
To: **< REDACTED >**
Cc: **< REDACTED > < REDACTED > < REDACTED > < REDACTED > < REDACTED >** Aston, Liz
Subject: Re: Urgent: exploitable vulnerability in Cellebrite / cyber kiosk systems [OFFICIAL]

Good afternoon everyone,

As mentioned earlier, here are a few “critical friend” concerns following on from the blog post. To be clear, the issue here is Cellebrite’s software, not Police Scotland’s use of it, so I appreciate that Police Scotland has essentially been thrown into this. So these questions are ones you should raise with Cellebrite, as they are the questions which occurred to us.
1. It appears from the blog that the software is wide open to attack from a phone being actively scraped, in such a way as evidence collected could easily be altered, damaged or added to. This could be used to challenge any reliance on the evidence collected by the software. Have you confirmed what steps Cellebrite are taking to address these issues?
2. How you will ensure your use of the software is kept secure in future? Does Police Scotland have any process for auditing evidential software for security issues?
3. The blog details apparent infringement of Apple’s copyright by Cellebrite. At a minimum, it leaves Cellebrite open to legal action from Apple at any time. This may cause Police Scotland to also be in violation of copyright law by retaining and using the software, or to have to cease using it in the event of legal action by Apple. The infringement would appear to be very hard to fix, as Cellebrite’s software seems reliant to these infringing components to function with Apple devices. Are Cellebrite taking steps to address this alleged infringement?
4. There is an implication in the blog that Signal have included defences for the products against scraping by Cellebrite. The nature of this won’t be known until it is encountered, but could range from disabling an extraction, to disabling the Cellebrite device entirely. Police Scotland should at a minimum seek clarification from Cellebrite on this, but is there a backup plan in place in the event that the Cellebrite system’s use needs to be suspended?
5. The blog highlights the sale and use of Cellebrite software in disreputable regimes. This is a concern in and of itself, but this publicity is likely to make it a continued target for cracking and circumvention. Given this, is Cellebrite willing to enhance the technical security and support they provide to Police Scotland?

Hope these are somewhat helpful.

Regards,
< REDACTED >

On 22 Apr 2021, at 11:31, Aston, Liz **< REDACTED >** wrote:

Thanks **< REDACTED >** it would be good to be kept updated on this when you know more.
< REDACTED > I'm sure that would be helpful -thank you.
From my basic in ititial understanding of the blog (I am not a technological expert but I think I understand some of the basic principles having been involved in the cyber kiosks ERG) the 'trojan horse' implications (at least initially) may not be as severe for cyber kiosks given that Police Scotland cyber kiosk machines are not networked but perhaps I am wrong and this will be different for the Cyber Hubs. However, there are many further questions raised which are of relevance to the work of the IAG, for example, in terms of the assessment of scientific

standards (re the security of celebrite) and many more.
Happy to discuss further as appropriate.
Thanks all
Liz

From: **< REDACTED >**
Sent: 22 April 2021 10:31
To: **< REDACTED >**
Cc: Aston, Liz; **< REDACTED > < REDACTED > < REDACTED > < REDACTED >**
Subject: Re: Urgent: exploitable vulnerability in Cellebrite / cyber kiosk systems [OFFICIAL]

CAUTION: This email originated from outside Edinburgh Napier University. Do not follow links or open attachments if you doubt the authenticity of the sender or the content.

Hi **< REDACTED >**,

Thank you for keeping us updated. I want to assure you that we will not make any media comments at this time.

In the interest of being a critical friend, we may send you a follow-up email later today with some secondary implications which could result from the initial disclosure.

Regards,
< REDACTED >

On 22 Apr 2021, at 10:17, **< REDACTED >** wrote:

OFFICIAL
Thanks Liz.

We will progress internally and keep you updated as appropriate.

I agree that comment at this stage is better avoided.

I will inform our comms teams and Cyber Security & Assurance teams who are responsible for our internal security & networks.
