EXPERT REVIEW

Review of the DPA B-Able "Samsung Mobile Vulnerability Risk Assessment", 30-1-2016

Case	
Name parties	Consumentenbond - Samsung

1 Details of the expert

Initials and last name	Prof. Dr ing. J.B.F. Mulder
Profession	Professor and CEO VIAgroep nv
Correspondence address	Patrijsweg 14
Telephone no	070-3368080
Fax no*	not applicable
Email address*	Hans.Mulder@Viagroep.nl

2 Details of the parties and their representatives

Party:

Name	Consumentenbond

Of claimant/petitioner/appellant

Representative:

(counsel or agent of the claimant/petitioner/appellant)

Name	SOLV Advocaten
Correspondence address	Anne Frankstraat 121, Amsterdam
Telephone no	020 530 0160
Fax no*	not applicable
Email address*	schimmel@solv.nl ; neervoort@solv.nl

Party:

Name	Samsung

[4] The *Practice Direction for experts in Dutch civil law cases* includes information on how to communicate with parties and their representatives.

(Counsel or agent of the defendant/respondent)

Name	Mr. Th. Conijn
Correspondence address	Olaf Palmestraat 10, 2616 LR Delft
Telephone no	015-2196161
Fax no*	not applicable
Email address*	t.conijn@samsung.com

3 Documents

Date of appointing the expert	16th December 2015, by Consumentenbond
Court documents of which the expert has taken note in view of the expert opinion	None
Other documents	None
Documents referred to in the opinion	Samsung Mobile Vulnerability Risk Assessment by DPA-B-Able B.V.
Documents disregarded by the expert	None
Reason	not applicable

4 Questions asked by the Consumentenbond

On Friday November 20th 2015 in consultation between mr. M. Fahmy of DPA B-Able, mr. Schimmel and mr. Neervoort of SOLV advocaten the questions were formulated regarding:

1. Determining Stagefright Leak on Samsung smart phones;
2. Determining Exploitation of vulnerabilities;
3. Patch Research, how complicated is it to patch the device?
4. Virus Scanner, do virus scanners offer a secure solution?

5 Set-up of the review

I have monitored and reviewed the research approach of DPA B-Able Mobile Vulnerability Risk Assessment. DPA B-Able has given the Consumentenbond the opportunity, prior to the examination, to make their own wishes relating to the examination known. Samsung the supplier of the smart phones is invited to attend to the research and comment on the report of DPA B-Able (see Practice direction for experts in Dutch civil law cases, nr. 27)

6 Answering the questions

6.1 Background

Mandated by the Consumentenbond DPA B-Able and prof. dr ing. Mulder have executed respectively monitored an investigation regarding the mobile vulnerability risks on Samsung smart phones. The Consumentenbond has provided the devices needed to be examined.

6.2 The expert's considerations

Because of the relevance of the findings of DPA B-Able mobile vulnerability risks assessment the expert answers the last question (‘de restvraag’: Heeft u nog overige opmerkingen die voor de beoordeling van de zaak van belang zouden kunnen zijn?)

6.3 Answers to the questions

Ad. 1. Determining Stagefright Leak

DPA B-Able has tested the Samsung smart phones, provided by the Consumentenbond on vulnerabilities. The tests were positive on 4-1-2016 for the Stagefright leak. During inspection at Samsung on 26-1-2016 and after updates the tests were negative, in other words the Stagefright vulnerabilities have been fixed in the latest update which was released earlier in January 2016 (see conclusions on page 5 of the DPA B-Able report).

Ad. 2. Determining Exploitation of vulnerabilities

DPA B-Able states at page 5: “There if no evidence at this time that the Stagefright vulnerability can be actively exploited on Samsung devices.”

Ad. 3. Patch Research, how complicated is it to patch the device?

DPA B-Able clarifies at chapter 4: “Google made the necessary patches for several vulnerabilities of Stagefright available within short notice… The speed at which Google patches are made available and the completeness … proves that it possible to provide older devices with the necessary patches”.

Ad. 4. Virus Scanner, do virus scanners offer a secure solution?

DPA B-Able states at page 12: “At the present, there are various products available that can provide good protection against one or more of the Stagefright vulnerabilities, examples of such products include Mobile protect from Trend Micro, Checkpoint Mobile Threat Prevention and Zimperium IPS (ZIPS) software. Making a choice between various products is very difficult for a consumer… The majority of the antivirus software on Android does not actively (permanently) protect against potential new leaks or sophisticated attacks”.

Ad. 5. Relevant findings of the DPA B-Able mobile vulnerability risks assessment
DPA B-Able states the following, page 4:

Samsung Security Patches process is not working at its optimum. The last update of January 2016 had fixed one of the exploitations namely Stagefright, other known vulnerabilities (e.g. Certifigate) were not fixed by these updates.

The interval between acknowledgement of a vulnerability and publishing an update which includes the patches is too long. This leads to the consumers being susceptible to high risks for a longer period of time.

Information presented on the website of Samsung regarding the security leaks, support time and information about devices is very vague.

7 The right of inspection and obstruction

1. the right of inspection and obstruction is applicable to this examination"	No (please go to 8)

8 The principle of equality of arms

1. inspection on location	0 yes: a. On Tuesday 26th January, location Samsung in Delft b. I gave the parties the opportunity to attend the inspection on location; c. the inspection on location was attended by Consumentenbond and Samsung
2. meeting(s) with parties	Not applicable (please go to 8.3)
3. medical examination of one party	Not applicable (please go to 8.4)

4. comments and requests[18]

a. by letter of 2-2-2016 I sent my opinion to the parties and in the letter provided them with the opportunity to make comments and requests before a date set by me.

b. I received the comments/requests from Samsung by e-mail of 8 February 2016 11:50

c. I received the comments/requests from De Consumentenbond by e-mail of 8 februari 2016 17:46

d. I have included the comments and requests as an annex to this expert opinion

e. my reply to the comments and requests[19]:

0 is stated under 9

[18] You are by law obliged to provide the parties with the opportunity to make comments and requests. Please consult, if necessary, the *Practice direction for experts in Dutch civil law cases.*

[19] In many cases it is clear to the court and the partjes if you leave your original opinion unchanged and separately respond to the comments and requests made by the parties. There is room to do so under 9.

9 Reply of expert to comments and requests

Van: Thomas Conijn <t.conijn@samsung.com>
Datum: maandag 8 februari 2016 11:50
Aan: "prof.dr. J.B.F. Mulder, 'Micha Schimmel | SOLV,
Frits.Gerritzen@allenovery.com
CC: 'Paul van Noesel', 'Martijn Kok', 'Mohamed Fahmy'
Onderwerp: RE: Consumentenbond - Samsung Mobile Vulnerability Risk Assessment

Dear Prof. Mulder,

Samsung has reviewed the draft report that was produced by DPA B-Able at the request of the Dutch Consumer Association (DCA).

The process and purpose of the investigation are unclear to Samsung. Therefore, Samsung will now respond in general terms, only. The report seems to consists mostly of the personal opinions of the two investigators. These opinions are mostly on legal questions that the DCA has put to the Judge of the Amsterdam Court in the course of preliminary relief proceedings. From the remarks of mr. Fahmy during the meeting at Samsung, it is clear that the investigators are by no means neutral or balanced. Finally, it seems that the questions that were apparently asked to the investigators by the DCA are not addressed in the report.

Samsung was notified on Wednesday 20 January 2016, by the DCA's attorney, that the DCA was planning to investigate some Samsung phones and that it invited Samsung to attend that investigation. Further to Samsung's request for an investigation set up and plan, Samsung received four questions from the DCA's lawyer that would be answered within the scope of the investigation. Subsequently a meeting was arranged at Samsung's offices on the 29th of January 2016 for – what Samsung had been told – the investigation into the four questions that had been put to the experts of DPA B-Able. Instead of addressing these questions, two Samsung phones (S5 mini & S5 Neo) were presented, switched on, and the Zimperium app was run. The app indicated the phones to be vulnerable for Stagefright. Subsequently the latest updates for both devices were installed and the Zimperium app was run again, and the devices turned out not to be vulnerable for any Stagefright vulnerability.

At no time during the meeting (or before that), did you or the investigators mention the Certifi-gate vulnerability. However that vulnerability is mentioned in the draft report.

I attended the meeting on behalf of Samsung and requested that the other three questions as presented would also be addressed, but I was told that that would not be necessary. Later on, however, it was mentioned that these questions would be part of the next phase of the investigation. I then asked to be provided with a plan for the investigation, so that Samsung could assess whether it would be willing to cooperate, and you agreed, with the consent of Mr. Schimmel, to provide that plan. However, that plan was never received and instead, Samsung was provided with a draft report from DPA B-Able on 2 February 2016, with the request to comment on that report.

I would like to stress again that Samsung does not subscribe to this investigation or the report in any way and that you have been appointed as a party witness for the DCA only.

I request that this response be included in the report in full.
Kind regards,
Thomas Conijn

Van: Micha Schimmel | SOLV <schimmel@solv.nl>
Datum: maandag 8 februari 2016 17:46
Aan: "prof.dr. J.B.F. Mulder", t.conijn@samsung.com",
"Frits.Gerritzen@allenovery.com"
CC: Paul van Noesel, Martijn Kok, Mohamed Fahmy, Marieke Neervoort | SOLV
Onderwerp: RE: Consumentenbond - Samsung Mobile Vulnerability Risk Assessment

Dear mr. Mulder,

As requested, please find attached the remarks of the Dutch Consumers' Association with regard to the Mobile Vulnerability Risk Assessment. Just as a gesture of courtesy I attach a separate document with a short list of apparent typos as well.

Best regards,

Micha Schimmel
Professional Support Lawyer

Remarks Dutch Consumers' Association

Expert review

On page 5 of the expert review, prof. Mulder answers the questions asked by the Dutch Consumers' Association. With regard to question number 2, he states that DPA B-Able states in its report: "There [is] no evidence at this time that the Stagefright vulnerability can be actively exploited on Samsung devices." The Dutch Consumers' Association would like to point out that the report of DPA B-able also states on page 5 of its report:
"This however, does not mean it is impossible that the vulnerability has already been exploited or can't easily be exploited in the short term. On Android devices from the Nexus line it has been demonstrated by various parties that exploitation of these vulnerabilities can occur."
In response to question 4, prof. Mulder states that there are various products available that can provide good protection against one or more of the Stagefright vulnerabilities. The Dutch Consumers' Association would like to point out that currently a Dutch consumer has no reasonable way of knowing whether his device is vulnerable to Stagefright or not. Even if one were to argue that all consumers have some form of virus scanner installed on their smartphone – which they don't – even then consumers would have no way of knowing which virus scanner would protect their smartphone adequately, since Samsung does not provide the required information.
In response to question 5, prof Mulder states that the Samsung security patch process is not working at its optimum. This requires some clarification, which can be found in the report of DPA B-Able. As stated on page 20 and onwards of the DPA B-Able report, the Samsung Galaxy S5 Neo is shipped with Android version 5.1.1, which version was vulnerable to Stagefright CVE's 2015-3876, 2015-3864 and 2015-6602. It is common practice to fix all known security vulnerabilities in software when providing a security update. However, when this smartphone received an update after first powering on the device, only two of these Stagefright CVE's were fixed, while CVE 2015-3876 was left open (DPA B-Able, page 28). For this reason, Samsung had to provide this smartphone with another update in the period between 4 January and 29 January. This shows that Samsung's update process is not functioning properly, and that puts consumers at risk.

DPA B-Able

On page 7 of the DPA B-Able report, the first question should not be whether Stagefright can be exploited, but where the Stagefright vulnerability is present on the tested smartphones.
On page 11 of the DPA B-Able report, it is stated that "[e]nabling Address Space Layout Randomization [...] makes abuse of Stagefright virtually impossible". The Dutch Consumers' Association would like to point out that Google's own security researchers have demonstrated that the way Android uses Address Space Layout Randomization is imperfect. Therefore, performing a successful exploit will take a bit more time, but will eventually be successful. Also interesting to note is that the result of an exploit attempt that failed due to ASLR is usually a crash of the smartphone, in some cases even a crash that normal consumers have no way of recovering from.

Response on questions and remarks of parties

In response to the questions and remarks of Samsung I confirm that I have been appointed as a party witness for the DCA only, and that as such the research set-up and questions were formulated in cooperation with the lawyers of the DCA.

I also confirm the remarks of the DCA as set out above:
On page 5 of the expert review, prof. Mulder answers the questions asked by the Dutch Consumers' Association. With regard to question number 2, he states that DPA B-Able states in its report: "There [is] no evidence at this time that the Stagefright vulnerability can be actively exploited on Samsung devices." The Dutch Consumers' Association would like to point out that the report of DPA B-able also states on page 5 of its report:
"This however, does not mean it is impossible that the vulnerability has already been exploited or can't easily be exploited in the short term. On Android devices from the Nexus line it has been demonstrated by various parties that exploitation of these vulnerabilities can occur."

In response to question 4, prof. Mulder states that there are various products available that can provide good protection against one or more of the Stagefright vulnerabilities. The Dutch Consumers' Association would like to point out that currently a Dutch consumer has no reasonable way of knowing whether his device is vulnerable to Stagefright or not. Even if one were to argue that all consumers have some form of virus scanner installed on their smartphone – which they don't – even then consumers would have no way of knowing which virus scanner would protect their smartphone adequately, since Samsung does not provide the required information.

In response to question 5, prof Mulder states that the Samsung security patch process is not working at its optimum. This requires some clarification, which can be found in the report of DPA B-Able. As stated on page 20 and onwards of the DPA B-Able report, the Samsung Galaxy S5 Neo is shipped with Android version 5.1.1, which version was vulnerable to Stagefright CVE's 2015-3876, 2015-3864 and 2015-6602. It is common practice to fix all known security vulnerabilities in software when providing a security update. However, when this smartphone received an update after first powering on the device, only two of these Stagefright CVE's were fixed, while CVE 2015-3876 was left open (DPA B-Able, page 28). For this reason, Samsung had to provide this smartphone with another update in the period between 4 January and 29 January. This shows that Samsung's update process is not functioning properly, and that puts consumers at risk.

10 Final invoice

1. has the financial invoice been enclosed?

0 no, after final report

2. has the specification of the final invoice been enclosed?

0 no, because

3. do you wish to receive Dutch VAT?

0 yes:

- the applicable VAT rate is 21 percent

0 over the entire amount of the final invoice

- the amount of the final invoice is

0 inclusive of VAT

11 Annexes

The following annexes are appended to this expert opinion:

DPA B-Able “Samsung Mobile Vulnerability Risk Assessment”, 30-1-2016

12 Signing the expert opinion

I send this opinion in duplicate to parties

Prepared on 10th February 2016 in The Hague

(signature)

(name)

Prof. Dr Ing. J.B.F. Mulder