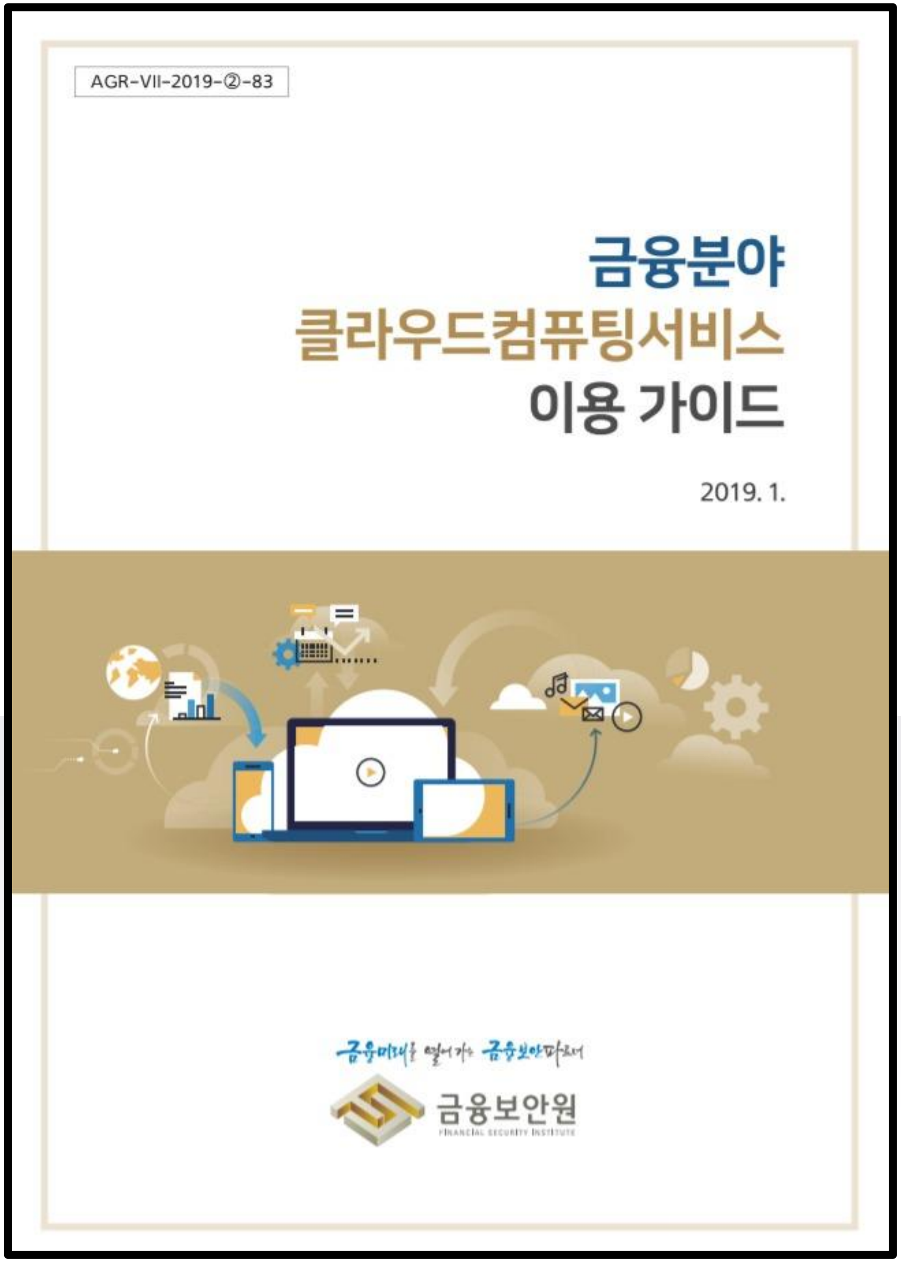
The Gap Between Cloud Service Providers And App Developers

고려대학교
사이버국방학과 · 정보보호대학원

대통령직속 4차산업혁명위원회

김 승 주 (Seungjoo Kim)
(Home) www.KimLab.net (Blog) www.Crypto.kr

Microsoft Azure
vmware
amazon web services
Google Cloud Platform
SOFTLAYER an IBM Company
ALERTLOGIC Security. Compliance. Cloud.
SECURITY-AS-A-SERVICE
Apps



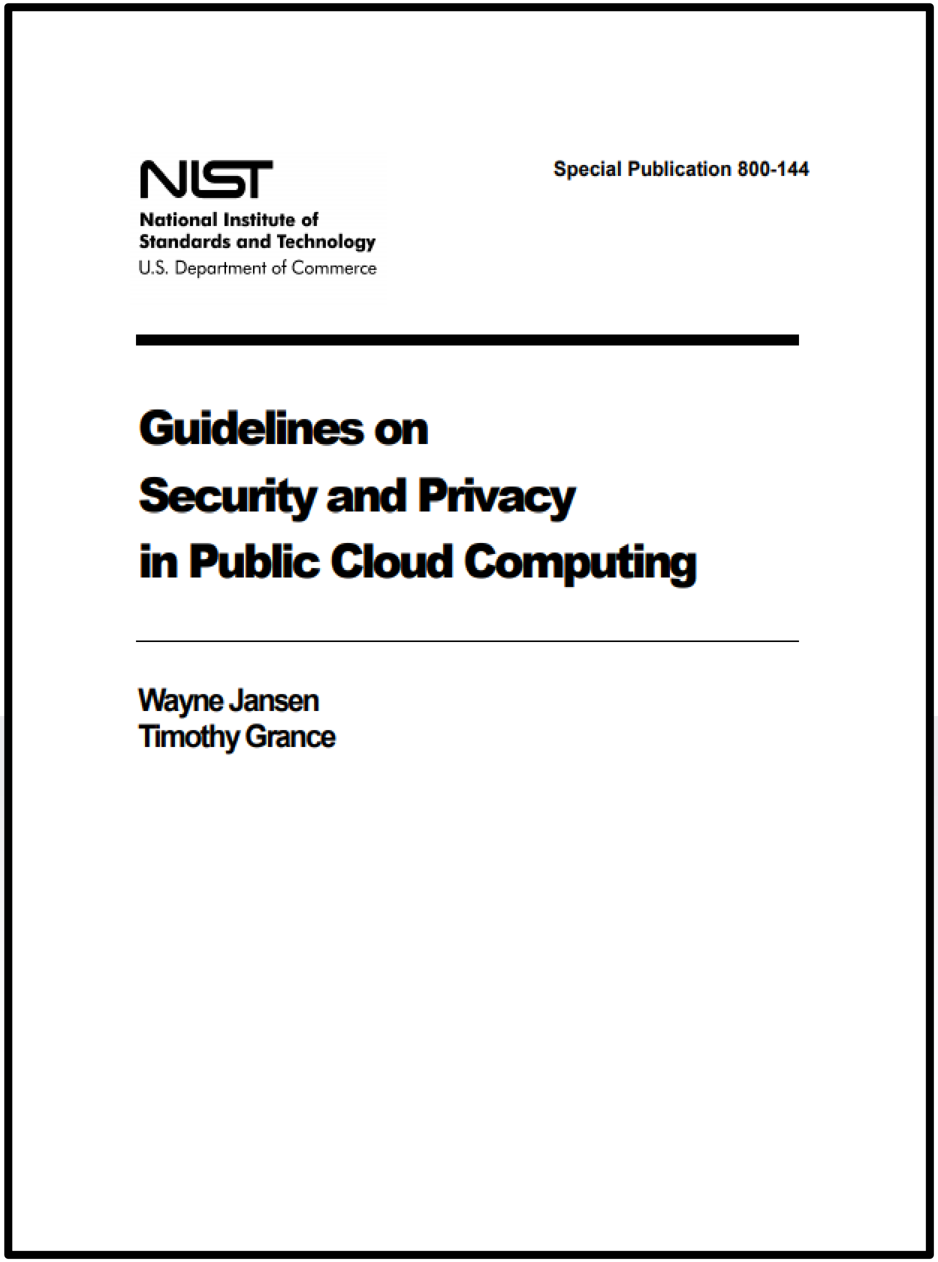
AGR-VII-2019-②-83

금융분야
클라우드컴퓨팅서비스
이용 가이드

2019. 1.

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

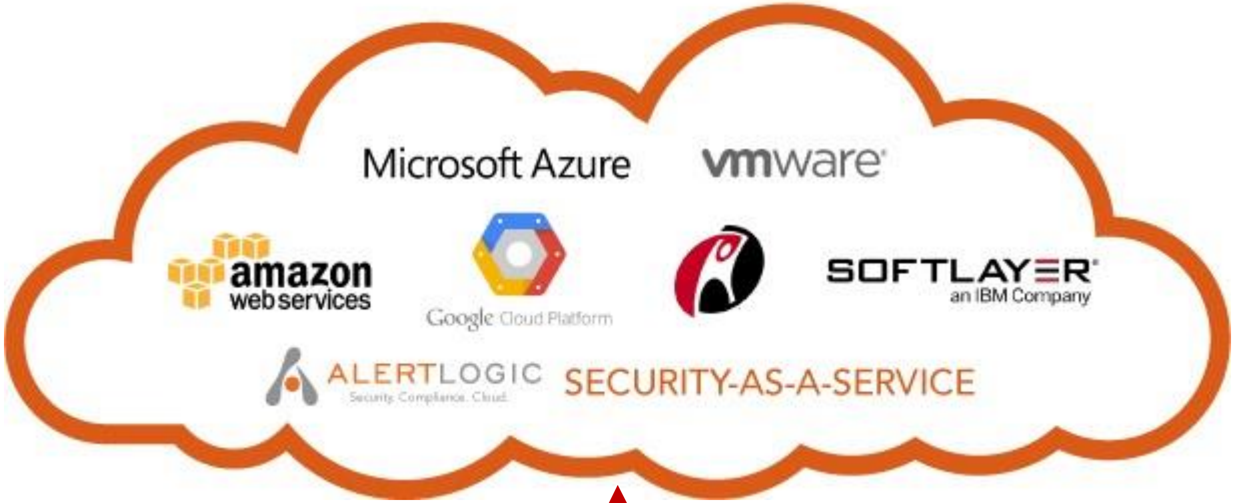


NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-144

Guidelines on
Security and Privacy
in Public Cloud Computing

Wayne Jansen
Timothy Grance



Microsoft Azure

vmware

amazon web services

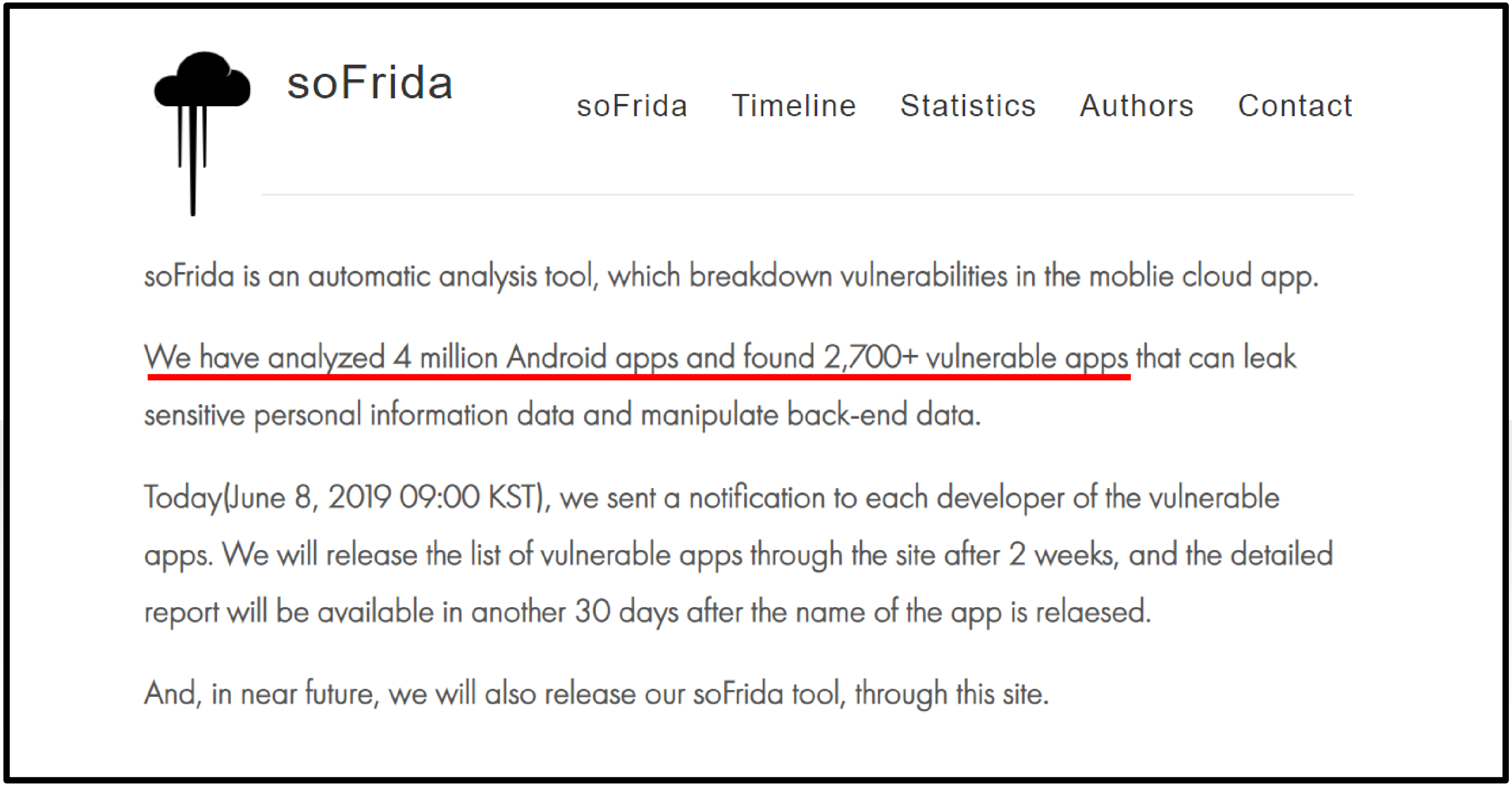
Google Cloud Platform

SOFTLAYER an IBM Company

ALERTLOGIC Security. Compliance. Cloud.

SECURITY-AS-A-SERVICE

soFrida.github.io

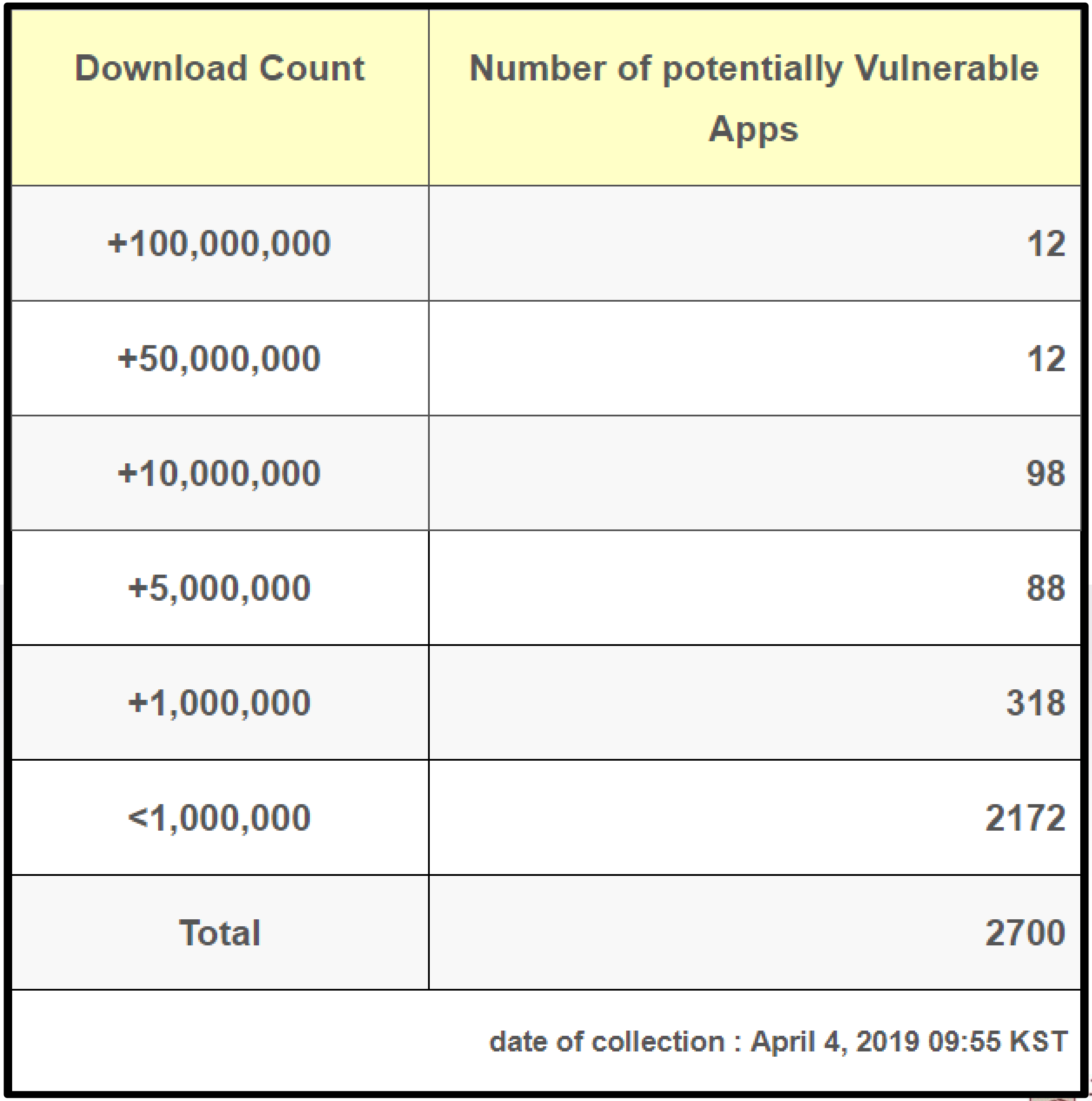


soFrida is an automatic analysis tool, which breakdown vulnerabilities in the moblie cloud app.

We have analyzed 4 million Android apps and found 2,700+ vulnerable apps that can leak sensitive personal information data and manipulate back-end data.

Today(June 8, 2019 09:00 KST), we sent a notification to each developer of the vulnerable apps. We will release the list of vulnerable apps through the site after 2 weeks, and the detailed report will be available in another 30 days after the name of the app is relaeased.

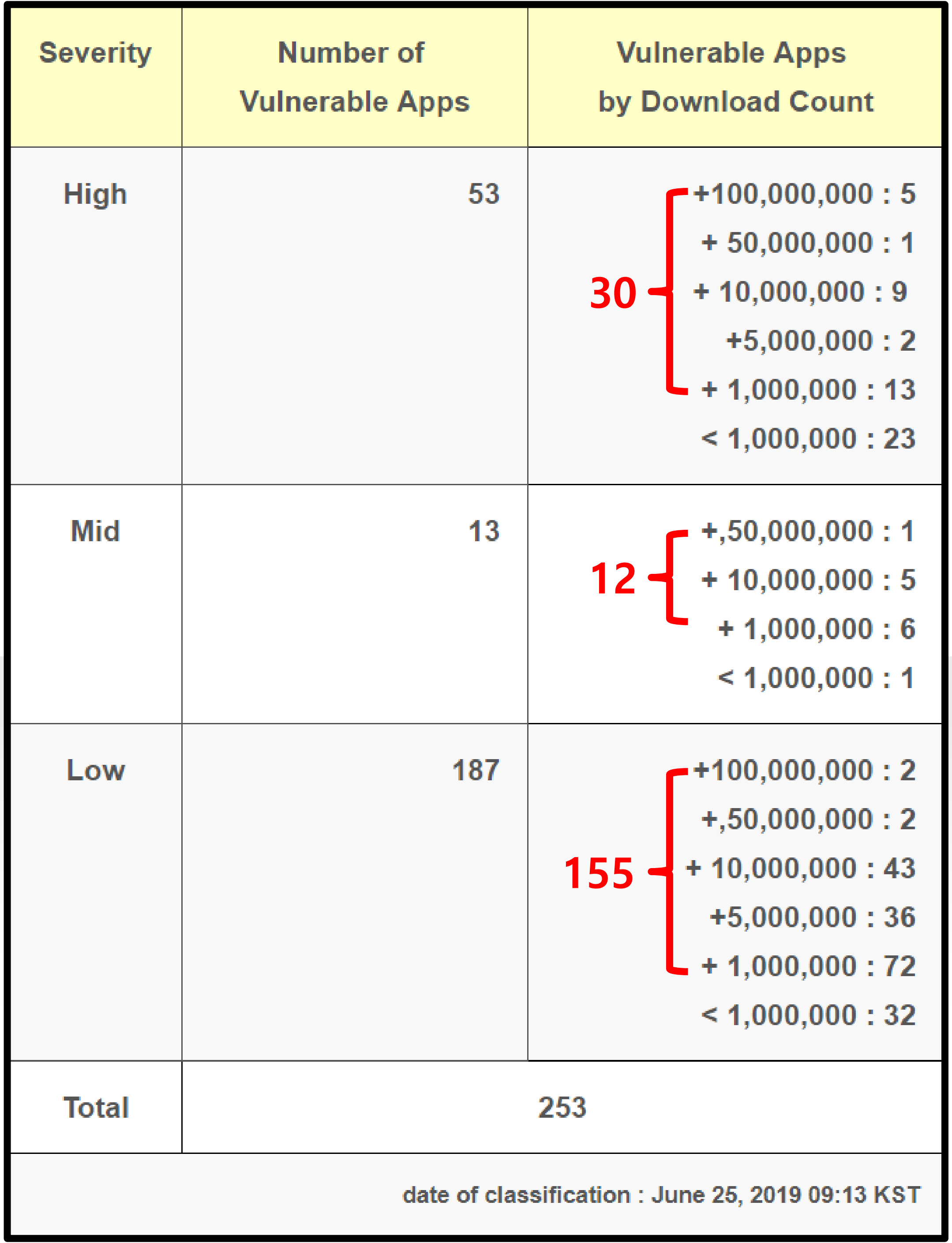
And, in near future, we will also release our soFrida tool, through this site.



Download Count	Number of potentially Vulnerable Apps
+100,000,000	12
+50,000,000	12
+10,000,000	98
+5,000,000	88
+1,000,000	318
<1,000,000	2172
Total	2700

date of collection : April 4, 2019 09:55 KST

528



Severity	Number of Vulnerable Apps	Vulnerable Apps by Download Count
High	53	30 +100,000,000 : 5 + 50,000,000 : 1 + 10,000,000 : 9 +5,000,000 : 2 + 1,000,000 : 13 < 1,000,000 : 23
Mid	13	12 +,50,000,000 : 1 + 10,000,000 : 5 + 1,000,000 : 6 < 1,000,000 : 1
Low	187	155 +100,000,000 : 2 +,50,000,000 : 2 + 10,000,000 : 43 +5,000,000 : 36 + 1,000,000 : 72 < 1,000,000 : 32
Total	253	

date of classification : June 25, 2019 09:13 KST

- **High :** An attacker can gain the unauthorized access to backend data or can manipulate data.
- **Mid :** The attacker have the limited access to backend data.
- **Low :** An attacker can't directly influence the app, but can collect some useful information or make an indirect service call.

Timeline

- **June 7, 2019**
  - We had identified **2,700+** android apps which were potentially vulnerable.
  - We began in-depth analysis of these 2700+ apps, and classified **236** apps as "actually risky".
- **June 8, 2019, 09:00**
  - We sent a **notification** to each developer of the vulnerable apps.

Timeline

- **June 18, 2019**
  - Through the in-depth analysis, **247** apps were classified as actually risky. (**11** apps added to the list of previously classified actually risky apps.)

- **June 19, 2019, 10:00**
  - We reported the vulnerability details and the list of vulnerable Korean apps to **KISA**, **NSR** and **FSI**.

Timeline

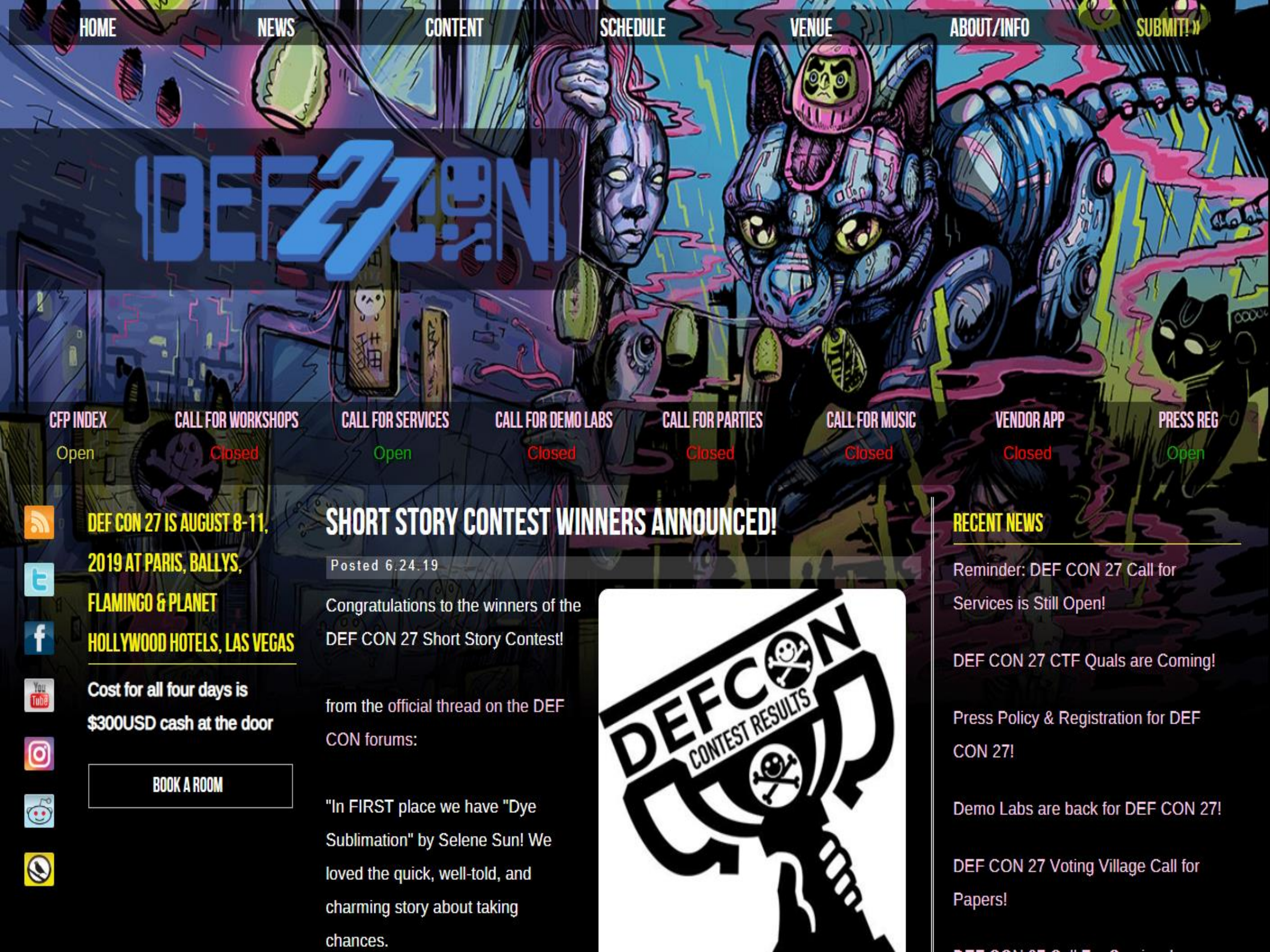
- **June 21, 2019, 03:37**
  - Among the developers we contacted, **only 3** developers contacted us again, so we had to take the following measures.
  - We contacted to security team of **Cloud Service Provider(CSP)** such as AWS, and asked them to help each app developer take an action.

Timeline

- **June 21, 2019, 16:23**
  - We had the **first response** from the security team of CSP.
- **June 25, 2019**
  - Through the in-depth analysis, **253** apps were classified as actually risky. (**6** apps added to the list of previously classified actually risky apps.)

Timeline

- **June 27, 2019 18:42**
  - CSP asked us to **hold publishing the list** of vulnerable apps.
  - As their request, we finally decided to delay publishing the list until they took enough action.



HOME NEWS CONTENT SCHEDULE VENUE ABOUT/INFO SUBMIT! »

CFP INDEX	CALL FOR WORKSHOPS	CALL FOR SERVICES	CALL FOR DEMO LABS	CALL FOR PARTIES	CALL FOR MUSIC	VENDOR APP	PRESS REG
Open	Closed	Open	Closed	Closed	Closed	Closed	Open

DEF CON 27 IS AUGUST 8-11, 2019 AT PARIS, BALLYS, FLAMINGO & PLANET HOLLYWOOD HOTELS, LAS VEGAS

Cost for all four days is $300USD cash at the door

BOOK A ROOM

SHORT STORY CONTEST WINNERS ANNOUNCED!

Posted 6.24.19

Congratulations to the winners of the DEF CON 27 Short Story Contest!

from the official thread on the DEF CON forums:

"In FIRST place we have "Dye Sublimation" by Selene Sun! We loved the quick, well-told, and charming story about taking chances.

RECENT NEWS

Reminder: DEF CON 27 Call for Services is Still Open!

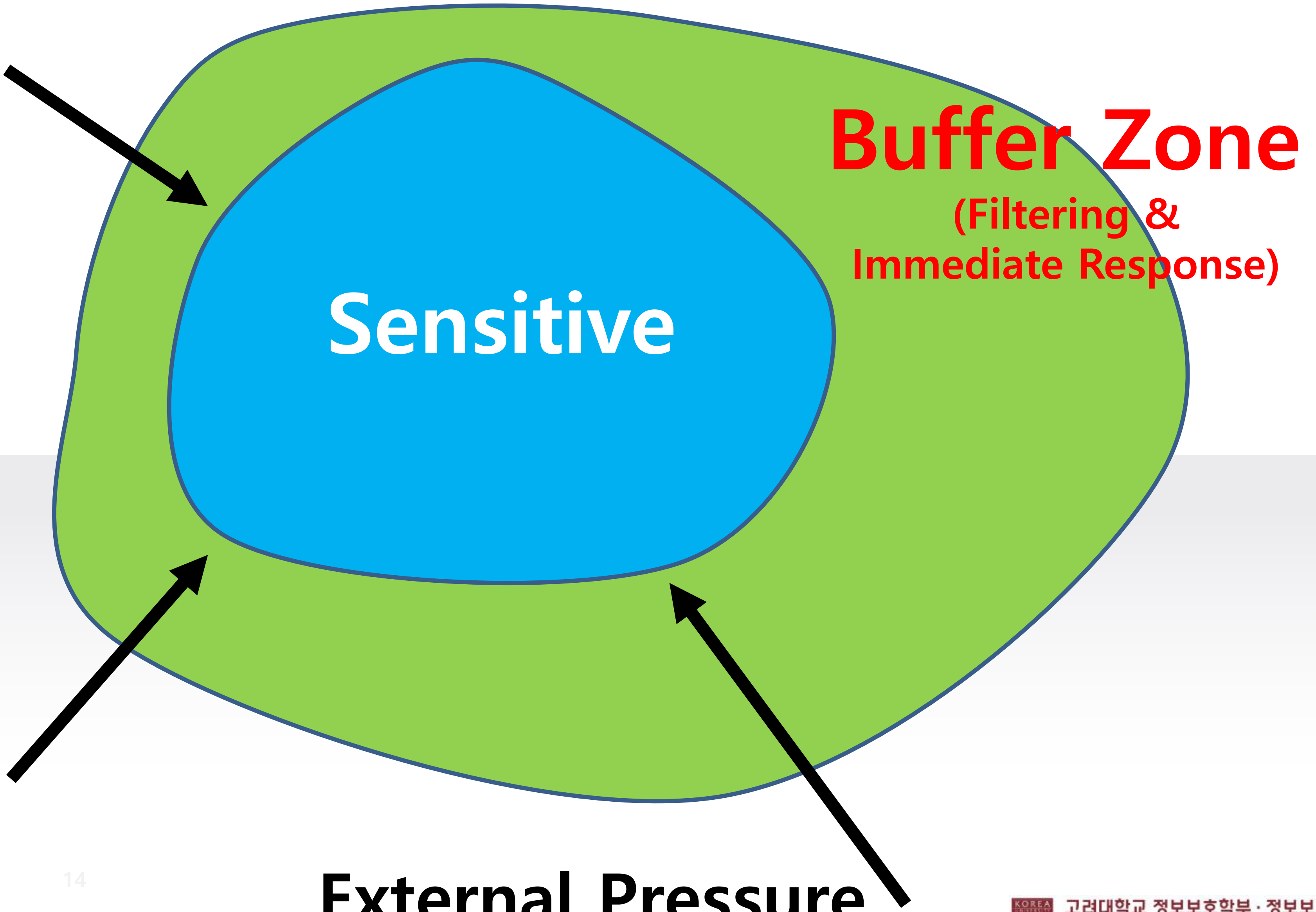
DEF CON 27 CTF Quals are Coming!

Press Policy & Registration for DEF CON 27!

Demo Labs are back for DEF CON 27!

DEF CON 27 Voting Village Call for Papers!

Conclusion



External Pressure

Akamai

The Gap Between Cloud Service Providers And App Developers

고려대학교

사이버국방학과 · 정보보호대학원

대통령직속 4차산업혁명위원회

김 승 주 (Seungjoo Kim)

(FB) www.fb.com/skim71 (Twitter) @skim71

고려대학교 정보보호학부 · 정보보호대학원
Korea University Division of Information Security
Graduate School of Information Security