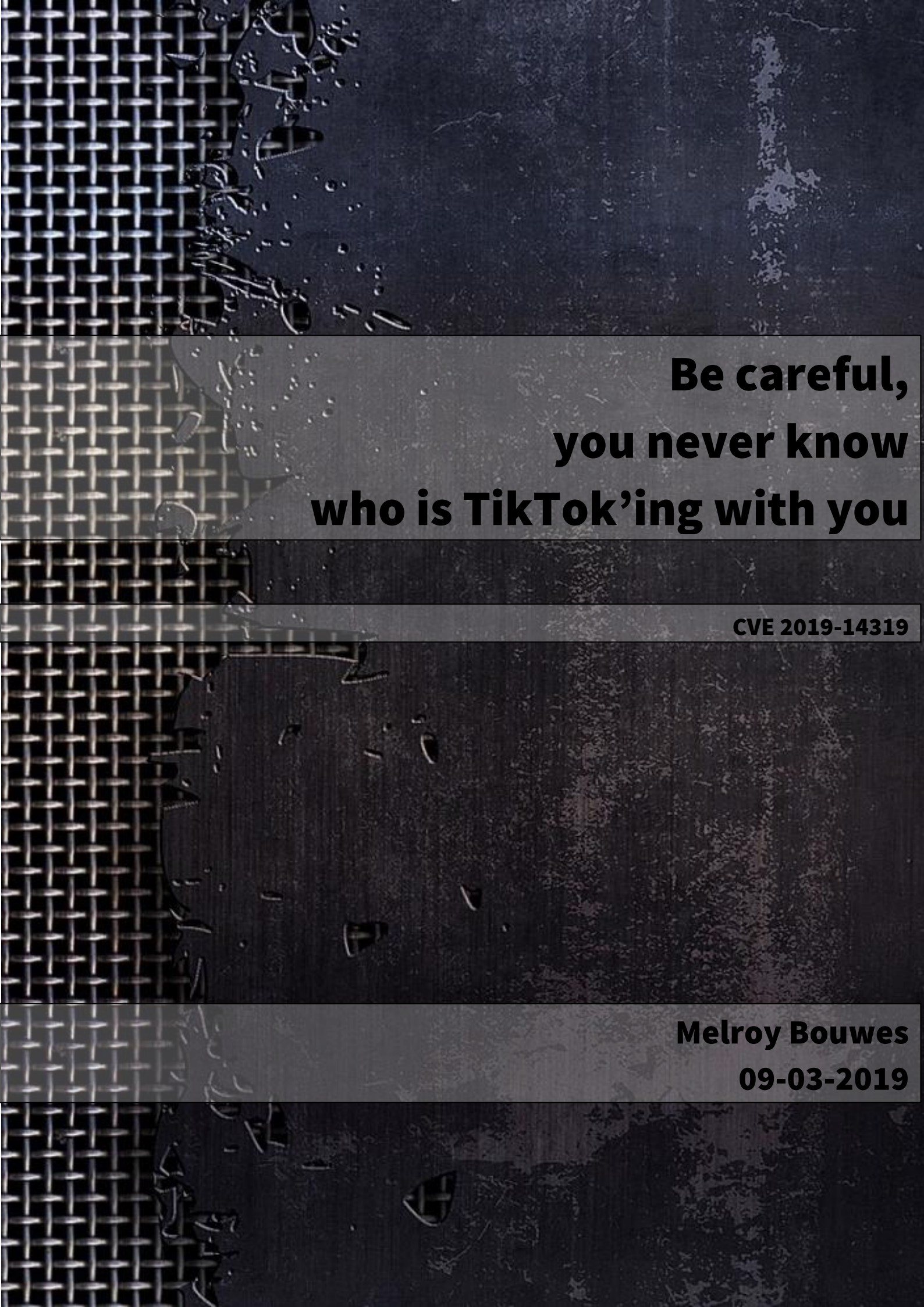


Be careful, you never know who is TikTok'ing with you

CVE 2019-14319

Melroy Bouwes

09-03-2019

Introduction

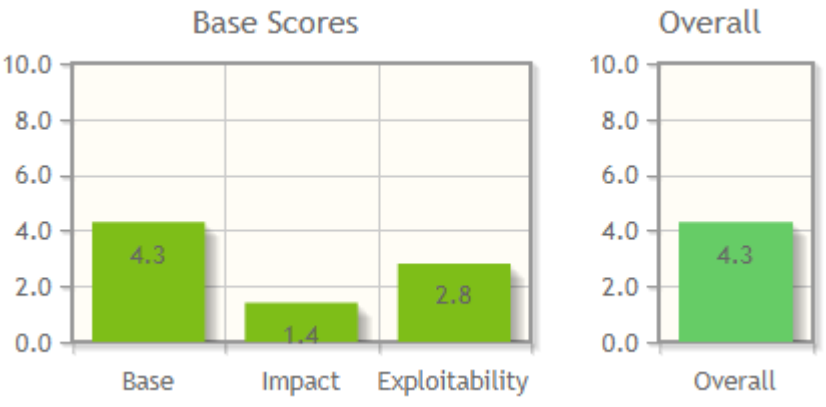
TikTok is the world's leading destination for short-form mobile videos. Their mission is to capture and present the world's creativity, knowledge, and moments that matter in everyday life. TikTok empowers everyone to be a creator directly from their smartphones, and is committed to building a community by encouraging users to share their passion and creative expression through their videos. TikTok has offices in Beijing, Berlin, Jakarta, London, Los Angeles, Moscow, Mumbai, Sao Paulo, Seoul, Shanghai, Singapore, and Tokyo. In 2018, TikTok was one of the most downloaded apps in the world. TikTok is available worldwide for iOS and Android.

They have no responsible disclosure process, they didn't respond to the mails with the finding in this report. . The following paper presents the research and its findings on both the TikTok Android and iOS versions.

Research

In my research I found a vulnerability enable a malicious attacker to spy on a TikTok user. This means the attacker can see the which movies the user is watching and collect information about the users device. This will compromise the user's privacy.

In order to carry out the attack, the attacker needs to be on the same Wi-Fi network as the user. This is possible via any public hotspot. Other scenarios where an attacker can intercept traffic include VPN or company administrators, DNS poisoning attacks or a malicious internet service provider - to name a few.



https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE 2019-14319 - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-14319

TikTok Versions

In the table are all the versions of the app i have tested:

Versions	
12.2.0	Vulnerable
12.3.0	Vulnerable
12.4.0	Vulnerable
12.5.0	Vulnerable
12.6.0	Vulnerable
12.6.1	Vulnerable
12.7.0	Vulnerable
12.8.0	Vulnerable

Attack Scenario

Both iOS and Android versions of TikTok make insecure HTTP requests when downloading user profile pictures and stills of the TikTok video. Attackers can easily discover what device is viewing which profiles/videos. Furthermore, information about the victim device information is readable for the attacker.

Use Cases

PHONE INFO

Highlighted in blue is the (unencrypted) HTTP POST request, the parameters contains information about the victim device that is running TikTok, in this example an Apple iPhoneX running iOS 13.1 with TikTok version 12.8.0 (Table for all info).

675	GET	200	HTTPS	api2.musical.ly	/passport/token/beat/?version_code=12.8.0&pass-region=1&pass-route=1&language…	application/json; c…	39
676	GET	200	HTTPS	api2-19-h2.musical.ly	/aweme/v1/user/settings/?version_code=12.8.0&pass-region=1&pass-route=1&langua…	application/json	1.133
677	GET	200	HTTPS	api2.musical.ly	/api/ad/splash/musical_ly/v15/?sdk_version=04915&version_code=12.8.0&language=e…	application/json	503
679	POST	200	HTTPS	t.appsflyer.com	/api/v4.9/iosevent?app_id=835599320&buildnumber=4.8.12	application/json	4
680	GET	200	HTTPS	api2-19-h2.musical.ly	/aweme/v1/abtest/param/?version_code=12.8.0&pass-region=1&pass-route=1&langu…	application/json; c…	2.946
682	POST	204	HTTPS	app-measurement.com	/a	image/gif	0
683	**POST**	**200**	**HTTP**	**mon.musical.ly**	**/monitor/collect/?version_code=12.8.0&pass-region=1&pass-route=1&la…**	**application/json…**	**180**
684	POST	200	HTTPS	log2.musical.ly	/service/2/app_log/?version_code=12.8.0&pass-region=1&pass-route=1&language=en…	application/json; c…	91
686	POST	200	HTTPS	xlog-va.musical.ly	/v2/r?os_ver=iOS%2013.1&os=1&app_ver=12.8.0&channel=App%20Store&ver=0.8.…	text/plain; charset…	83

http://mon.musical.ly/monitor/collect/?version_code=12.8.0&pass-region=1&pass-route=1&language=en&app_name=musical_ly&vid=A8A0054E-9C84-4755-A18F-063909BD4BB6&app_version=12.8.0&carrier_region=NL&is_my_cn=0&channel=App%20Store&mcc_mnc=20408&device_id=6716432008921548294&tz_offset=7200&account_region=NL&sys_region=NL&aid=1233&residence=NL&screen_width=1125&uoo=0&openudid=63c5c0b256155fdb6fa3b086099ed21190e0fed3&os_api=18&ac=WIFI&os_version=13.1&app_language=en&tz_name=Europe/Amsterdam&current_region=NL&device_platform=iphone&build_number=128009&device_type=iPhone10,6&iid=6732358480658941701&idfa=88C615E1-E48C-4D90-B5A1-DE601BD138FF

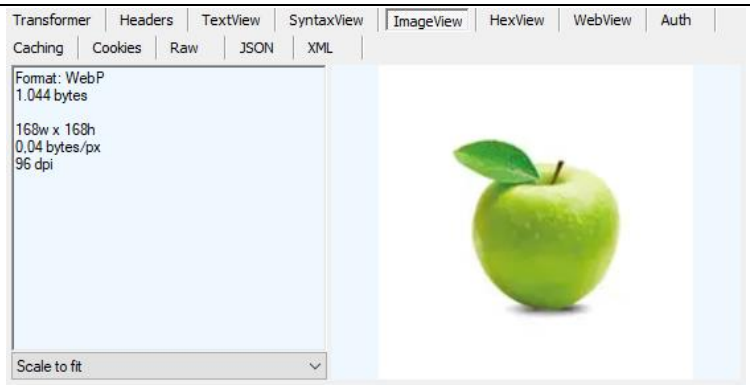
Name	Value	Comment
version_code	12.8.0	
pass-region	1	
pass-route	1	
language	en	Device Language (English)
app_name	musical_ly	
vid	A8A0054E-9C84-4755-A18F-063909BD4BB6	
app_version	12.8.0	
carrier_region	NL	
is_my_cn	0	
channel	App Store	
mcc_mnc	20408	Provider (NL KPN)
device_id	6716432008921548294	
tz_offset	7200	TimeZone (GMT +2)
account_region	NL	
sys_region	NL	
aid	1233	
residence	NL	
screen_width	1125	Screen Wiidt in Pixels
uoo	0	
openudid	63c5c0b256155fdb6fa3b086099ed21190e0fed3	
os_api	18	
ac	WIFI	Connection
os_version	13.1	iOS version
app_language	en	
tz_name	Europe/Amsterdam	
current_region	NL	
device_platform	iphone	
build_number	128009	
device_type	iPhone10,6	Device Model (iPhoneX)
iid	6732358480658941701	
idfa	88C615E1-E48C-4D90-B5A1-DE601BD138FF	Identifier For Advertising

PROFILE PICTURES

Highlighted in blue is the (unencrypted) HTTP GET request, the URL is directing to the user profile picture (.webp format) of the video that is requested by the victim.

756	GET	200	HTTP	p16.muscdn.com	/img/musically-maliva-obj/1643303235086342~c5_168x168.webp	image/webp	2.706
757	GET	200	HTTP	p16.muscdn.com	/img/tos-maliva-p-0068/ef62716d13954e23be4714ec15f55374~noop.image	image/jpeg	40.539
758	GET	200	HTTP	p16-tiktokcdn-com.aka...	/aweme/100x100/tiktok-obj/1643239353310210.webp	image/webp	5.844
759	POST	200	HTTPS	api2-19-h2.musical.ly	/aweme/v1/aweme/stats/?version_code=12.8.0&pass-region=1&pass-route=1&langua...	application/json; c...	141
760	**GET**	**200**	**HTTP**	**p16.muscdn.com**	**/img/musically-maliva-obj/1643581206805510~c5_168x168.webp**	**image/webp**	**1.044**
761	GET	200	HTTP	p16.muscdn.com	/img/musically-maliva-obj/1643581206805510~c5_100x100.jpeg	image/jpeg	1.497
762	GET	200	HTTP	p16-sg.muscdn.com	/large/v0201/5dee45746b6f409c9cb439cf29db5beb.jpeg	image/jpeg	63.458
763	POST	200	HTTPS	api2-19-h2.musical.ly	/aweme/v1/aweme/stats/?version_code=12.8.0&pass-region=1&pass-route=1&langua...	application/json; c...	140
764	GET	200	HTTP	p16-tiktokcdn-com.aka...	/img/tiktok-obj/1635811587407874~c5_168x168.webp	image/webp	6.960

http://p16.muscdn.com/img/musically-maliva-obj/1643581206805510~c5_168x168.webp



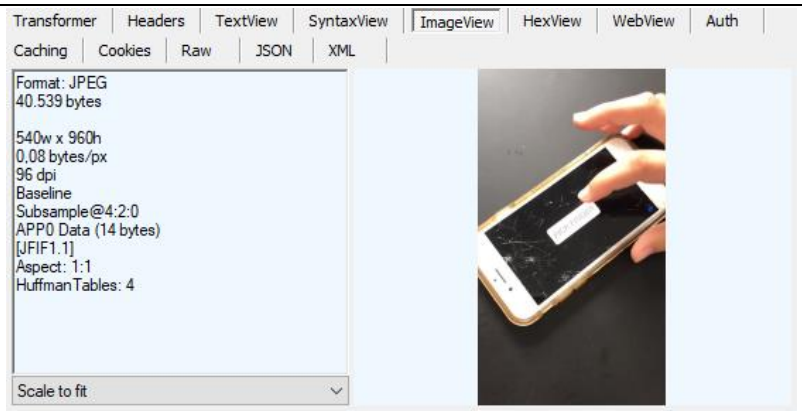
User Profile picture in Fiddler

VIDEO STILLS

Highlighted in blue is the (unencrypted) HTTP GET request, the URL is directing to video still (.jpeg format) of the video that is requested by the victim.

751	GET	200	HTTP	p16.muscdn.com	/img/tos-maliva-p-0068/d56b2d792e9e48758505c35e0682fe4d~noop.image	image/jpeg	67.651
753	POST	200	HTTPS	api2-19-h2.musical.ly	/aweme/v1/aweme/stats/?version_code=12.8.0&pass-region=1&pass-route=1&langua...	application/json; c...	134
756	GET	200	HTTP	p16.muscdn.com	/img/musically-maliva-obj/1643303235086342~c5_168x168.webp	image/webp	2.706
757	**GET**	**200**	**HTTP**	**p16.muscdn.com**	**/img/tos-maliva-p-0068/ef62716d13954e23be4714ec15f55374~noop.ima...**	**image/jpeg**	**40.539**
758	GET	200	HTTP	p16-tiktokcdn-com.aka...	/aweme/100x100/tiktok-obj/1643239353310210.webp	image/webp	5.844
759	POST	200	HTTPS	api2-19-h2.musical.ly	/aweme/v1/aweme/stats/?version_code=12.8.0&pass-region=1&pass-route=1&langua...	application/json; c...	141
760	GET	200	HTTP	p16.muscdn.com	/img/musically-maliva-obj/1643581206805510~c5_168x168.webp	image/webp	1.044

http://p16.muscdn.com/img/tos-maliva-p-0068/ef62716d13954e23be4714ec15f55374~noop.image



Video Still in Fiddler

Recommendations:

I highly recommend switching HTTP to HTTPS. One might argue that this affects speed quality, but when it comes to the privacy and sensitivity needed, speed should not be the main concern.

At least Phone/Device Information needs to be encrypted.

Contact Details

Melroy Bouwes
Melroy.bouwes@outlook.com