U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0007

TIKTOK SECURITY CONCERNS & DATA HARVESTING

DATE ISSUED: 9th July 2020

IMPACT	LOW	[✓ MEDIUM]	HIGH
EASE OF EXPLOIT	[✓ LOW]	MEDIUM	HIGH

OVERVIEW

TikTok poses a number of security risks through the use of APIs to collect data on users personal and device information and includes capabilities for remote logging, configuration and file downloads.

BREAKDOWN

Information is collected by a local proxy installed on your device within the application for “transcoding media” whereby all logging activities are able to be configured remotely and has no authentication process so is easily exploitable. TikTok has protections are in place to prevent users from debugging or reversing the application, restricting functionality where this is attempted or other services access permissions are denied. Android versions of the application include the capability to download, unzip, install and execute files remotely. Previously user PII data was leaked through the HTTP REST API and TikTok have recently been fined for illegally collecting children’s data. A number of organizations have banned employees from using the application. Information harvested can include:

Phone hardware:	CPU type and number, hardware IDs, screen dimensions, memory usage, disk space, etc.
Network related:	IP address, Local IP address, router MAC, device MAC, Wireless Access Point SSID, etc.
Other:	Other applications installed, rooted or jailbroken device status,

REMEDIATION STEPS

- Remove TikTok application from all devices containing any sensitive information
- Block the TikTok application from company networks and resources

REFERENCES & RESOURCES

Bored Panda:	https://www.boredpanda.com/tik-tok-reverse-engineered-data-information-collecting/?utm_source=linkedin&utm_medium=social&utm_campaign=organic
Cyber Scoop	https://www.cyberscoop.com/tiktok-dnc-security-concerns/
Tripwire	https://www.tripwire.com/state-of-security/security-data-protection/tiktok-fined-5-7m-for-illegally-collecting-personal-data/?web_view=true