SNOOPWALL
FLASHLIGHT APPS THREAT ASSESSMENT REPORT

Summarized Privacy and Risk Analysis of Top 10 Android Flashlight Apps
by SnoopWall mobile security experts and the Privacy App scanner

THREAT REPORT

Flashlight Apps	Super-Bright LED Flashlight	Brightest Flashlight Free	Tiny Flashlight + LED	Flashlight	Flashlight	Brightest LED Flashlight	Color Flashlight	High-Powered Flashlight	Flashlight HD LED	Flashlight: LED Torch Light
Permissions										
retrieve running apps	✓					✓		✓		
modify or delete the contents of your USB storage	✓	✓				✓		✓		
test access to protected storage	✓	✓				✓		✓		
take pictures and videos	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
view Wi-Fi connections	✓	✓				✓		✓	✓	
read phone status and identity	✓	✓			✓	✓		✓		
receive data from Internet	✓					✓		✓		
control flashlight	✓	✓	✓			✓	✓	✓	✓	
change system display settings	✓					✓		✓		
modify system settings	✓					✓		✓		
prevent device from sleeping	✓	✓	✓	✓		✓		✓	✓	✓
view network connections	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
full network access	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
approximate location (network-based)	✓	✓						✓		
precise location (GPS and network-based)	✓	✓						✓		
disable or modify status bar	✓	✓								
read Home settings and shortcuts	✓	✓		✓						✓
install shortcuts	✓	✓		✓						✓
uninstall shortcuts	✓	✓		✓						✓
control vibration	✓		✓							
write Home settings and shortcuts				✓						✓
disable your screen lock				✓						✓
read Google service configuration					✓				✓	

THREAT REPORT RECOMMENDATIONS

We've come up with a list of what we think are best practices for increasing privacy and security on your device without spending any money. This is based on SnoopWall's counterveillance research for improving your privacy from eavesdroppers and helping you from getting infected with spyware that could cost you your identity. They are:

1. Disable your GPS at all time except in an emergency or when you need to use your smartphone for navigation purposes;

2. Disable your NFC (Near Field Communications) or on Apple devices, iBeacon, unless you need them enabled for critical applications (http://support.apple.com/kb/HT6048);

3. Disable Bluetooth at all times except when you are in your car, driving, if you want to have hands-free calls, if supported by your car;

4. Verify Apps behavior and privacy risk BEFORE installing – do some research and ask the questions "why does this app need GPS, MICROPHONE, WEBCAM, CONTACTS, etc.?" – most apps don't need these ports unless they want to invade your privacy. Find an alternative before installing risky Apps;

5. Either put masking tape over your webcam and microphone when not in use or pull the battery out of your smartphone when you are not using it.

Obviously for #1, there's no need for geolocating you, unless you don't mind being spied upon by

these malicious flashlight apps – or worse – your children's location being monitored by online predators. Best to keep this hardware port disabled until you really need it.

For #2, you're probably wondering "what the heck is NFC and why should I care?". We'll it's a new protocol for 'bumping' or getting close to other devices, within 3 meters or so, to exchange information such as photos and contacts. Is it secure? No. Can it be hacked just like Bluetooth? Yes. Go into your device settings, find NFC, if you see it, disable it.

Ok, for #3, you're thinking 'that makes sense' – Bluetooth is an easily hacked protocol and folks can eavesdrop on communications over Bluetooth; broadcast into your earpiece (yes, it's been done); access your contacts list and hack your smartphone device over Bluetooth. So, if you disable this protocol everywhere except when you are in the car, wanting a hands free experience for making and receiving calls, you should be much more secure.

For #4, how many times do you install an app with excitement about promised features and functions, only to find that it requires incredible privacy risk? If it's too good to be true it probably is and nothing in this world is free. There are 9 major advertisement networks and some deploy spyware. Free apps use these networks to monetize their businesses and some are developed by professional cyber criminals, enemy nation states for spying or by hackers for malicious reasons.

We really don't like making recommendation #5 but until you try out our SnoopWall product, there's really nothing you can do to block webcam and microphone eavesdropping, so why not make it hard for the bad guys to see or hear anything useful?

SOLUTION:

Some of the Flashlight Apps write settings and have access to your device storage; it may be to install additional backdoors or remote access Trojans (RATs). Therefore you might need to reset your phone completely after an uninstall of your favorite Flashlight App. Some might even wish to go to FACTORY RESET or a WIPE. Once you've cleaned off the Flashlight RAT, you might still want a flashlight app on your phone that you can trust.

What about Apple iPhone and iPad or Microsoft WindowsPhone flashlight apps?

The flashlight app pre-installed on the Apple iPhone appears to be safe.

However in both the iTunes store and on the Windows Phone app store, 3rd party flashlight apps access various hardware ports. The ports they access while they are running includes Webcam, Location Services, using your GPS and other coarse location based internet. In addition, they use your internet connection.

The good news is that on these two operating systems apps like this cannot hide in the background.

The bad news is when you run downloaded Flashlight Apps on these two platforms, they are still building up a profile on users including your location, and are able to send and receive information over the internet – totally unnecessary for a flashlight.

WARNING: Don't reset or wipe without backing up ONLY those contacts and files you are certain to trust. If you do a complete device backup and restore, you risk also restoring malware. Ask a friend who is an expert with your kind of phone or the staff at the store you purchased your smartphone or tablet on how to do this the right way.

UNINSTALLATION INSTRUCTIONS for Android Apps:

1. Visit your device's Settings menu > Apps or Application manager (this may differ depending on your device).
2. Touch the app you'd like to uninstall.
3. Select Uninstall.

We developed the SnoopWall Privacy Flashlight for Google Android, Apple iOS and Microsoft Windows smartphones and tablets. The file size of the SnoopWall Privacy Flashlight application is approximately 72 kilobytes. It only accesses the light of the webcam and the screen display which is all a flashlight app should be doing anyway. Get it today at: http://privacyflashlight.snoopwall.com

We've also developed another free application called Privacy App which will scan your Android or Windows device and show you which apps are spying on you. If you have suspicions, confirm them with Privacy App. Learn more about our technology and products at: http://www.snoopwall.com/products/

END OF REPORT.

About Gary Miliefsky
Counterveillance expert and founding member of the U.S. Department of Homeland Security, Gary Miliefsky, is the Founder of SnoopWall and the sole inventor of the company's technologies. He has successfully advised two White House administrations on cyber security, filed more than a dozen patents of his network security inventions, and licensed technology to major public companies, including IBM, BlackBox Corp. and Computer Associates International. Gary is a recent Editor of Cyber Defense Magazine. He also founded NetClarity, Inc., an internal intrusion defense company, based on a patented technology he invented. He also advised the National Infrastructure Advisory Council (NIAC) at the U.S. Department of Homeland Security, in their development of The National Strategy to Secure Cyberspace. Miliefsky serves on MITRE's advisory board and its CVE Program (http://CVE.mitre.org) and is a founding Board member of the National Information Security Group (www.NAISG.org). He is a member of ISC2.org, CISSP® and Advisory Board of the Center for the Study of Counter-Terrorism and Cyber Crime at Norwich University. Gary is a prolific author, a frequent presenter and subject matter expert on topics related to digital privacy, counterveillance and cybersecurity for corporations and the news media.

About SnoopWall
SnoopWall is the world's first counterveillance software company focused on helping consumers and enterprises protect their privacy on all of their computing devices including smartphones, tablets, and laptops. SnoopWall augments endpoint security (antivirus, firewall, intrusion prevention) through patent-pending technology that detects and blocks all remote control, eavesdropping and spying, thereby preventing data leakage while increasing device battery life/performance. SnoopWall's technology suite includes Privacy App ™ and Privacy Shield ™. SnoopWall's software is proudly made in the U.S.A. and is part of the growing suite of next generation security products being delivered by SnoopWall and their OEM partners. Visit snoopwall.com and follow us on Twitter: @SnoopWallSecure.

Media Contact:
pr@snoopwall.com
1-800-991-3871

Address:
SnoopWall LLC
One Tara Boulevard, Suite 200
Nashua, NH - 03060
Phone: 1-800-991-3871
E-mail: sales@snoopwall.com