MEDIA ALERT: BugSec, Cynet Uncover SNAP, a Major Vulnerability on LG G3 Devices

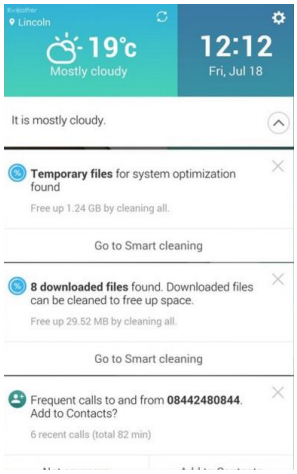
Millions of LG Smartphones Could Be Hijacked, Personal Data Breached

TEL AVIV, ISRAEL — Thursday, January 28, 2015

BugSec Group Ltd., a leading provider of cyber security services (www.bugsec.com), and Cynet, pioneers of the all-in-one agentless solution for detection and remediation of advanced and unknown threats (www.cynet.com), announced today that a joint team of researchers has discovered a severe security vulnerability in LG G3 Android devices, enabling the potential hijack of an estimated 10 million smartphones worldwide.

'SNAP' is a smartphone vulnerability that allows an attacker to run arbitrary JavaScript code on the devices, which can easily lead to private data leakage, phishing attacks and to denial of service (DOS) on the device.

The SNAP vulnerability, first discovered by team security researchers Liran Segal and Shachar Korot, is a flaw in one of the pre-installed LG applications, Smart Notice, which exists on every new LG G3 device. Smart Notice displays recent notifications to users that can be forged to inject unauthenticated malicious code. The application is on default work state.



Using the vulnerability, an attacker can easily steal sensitive data from the device SD card, including WhatsApp data and images, and can also mislead the end-user into phishing scams and drive-by attacks.

We commend LG, which responded quickly to our discovery of the vulnerability and we encourage users to upgrade their application to the new Smart Notice release, which contains a patch.

To see full details of the vulnerability, read the blogpost at www.bugsec.com/news/snap-attack-lg or www.cynet.com/snapattack1.

"LG reacted immediately, which we appreciate," said Idan Cohen, BugSec's Chief Technology Officer. "This is a major potential security breach into the personal data of millions of LG users worldwide." The root cause behind the issue, Cohen said, is the fact that the Smart Notice application does not validate the data it presents to users. "This means that the data can be taken from device phone contacts and manipulated. We highly recommend G3 users install the patch without delay," Cohen said.

The BugSec-Cynet security research team found that hijacking of the LG devices could essentially take place in several ways, based on the functionality issues of the Smart Notice application. The following scenarios, in which the application pops notifications (named 'cards') are all potential breaches:

- Favorite contact notifications – Recommend user keeps in touch with favorite contacts.
- New contact suggestions – Suggest saving a caller number.
- Callback reminders – Reminder to callback a contact after declining the call.
- Birthday notifications – Reminder about contact birthday.
- Memo reminders – Provide notifications about user memos.

To get expert advice on cyber-attack simulation and penetration testing, contact BugSec at info@bugsec.com.

To learn more about detection of unknown threats, contact Cynet at info@cynet.com.

About BugSec

BugSec Group is a leading offensive security consulting company, focused on ethical hacking, security research, cyber-attack simulations, SCADA, Incident Response, product security evaluation and other services to increase customer security. Since 2005, BugSec has been providing security consulting services to global companies in

the fields of finance, defense, government, hi-tech, utilities and other markets. The BugSec team is made up of some of the world's most talented offensive and defensive hacking experts and security research teams, who work together with intelligence and law enforcement organizations around the world to help our customers protect their assets.
www.bugsec.com

Follow BugSec at:
Facebook: www.facebook.com/BugSec-121433554543115/
Twitter: www.twitter.com/bugsec_group
LinkedIn: www.linkedin.com/bugsec

About Cynet
Cynet is a pioneer of the all-in-one, agentless solution for detection and remediation of advanced and unknown threats, such as unsigned malware and zero day attacks. The company's flagship product, Cynet 360, correlates and analyzes indicators from files, network, endpoints and user behavior to uncover threats, which have bypassed the prevention layer. Cynet's integrated 24/7 SOC ensures the validity of threats, assisting customers with remediation while eliminating false positives. www.cynet.com

Follow Cynet at:
Facebook: www.facebook.com/cynet360
Twitter: www.twitter.com/cynet360
LinkedIn: www.linkedin.com/cynet-security

Press Contacts:
Inbal Aharoni
Marketing Manager
Mobile: +972-508776797
Email: inbala@cynet.com

David Leichner
VP Marketing & Sales
Mobile: +972-547799888
Email: davidl@cynet.com

####