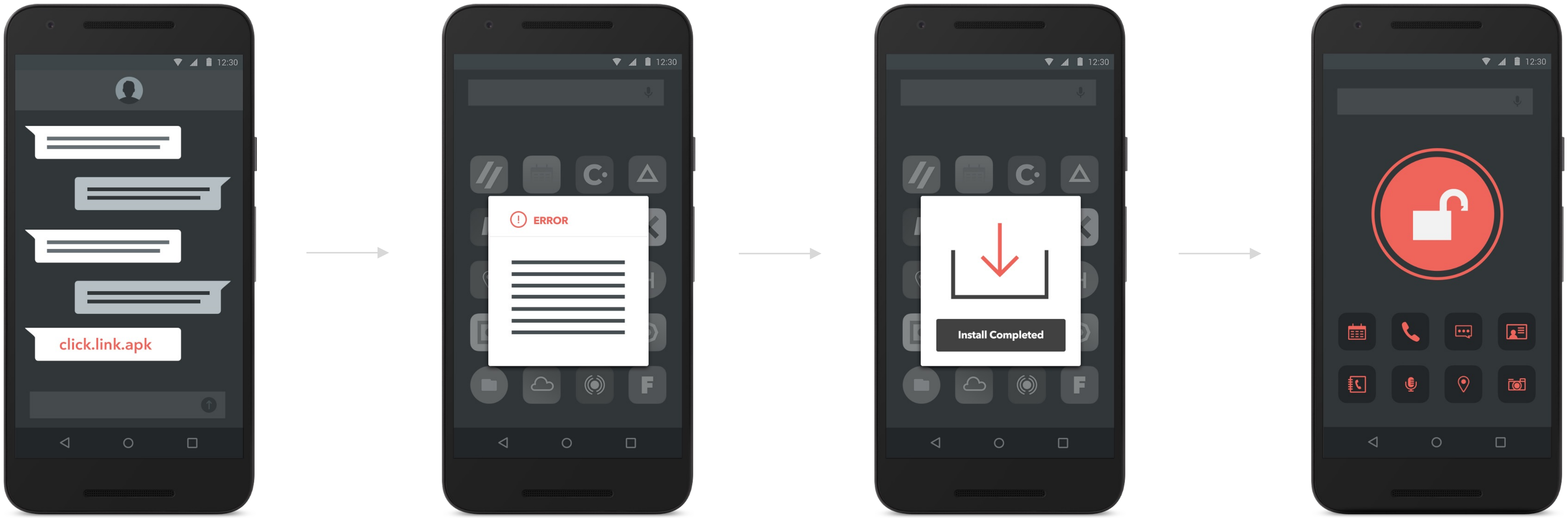
Lookout™

Access42 CyberSecurity Summit 2023

15. June 2023

Sascha Spangenberg

Mobile Kill Chain starts with a click



Social Engineer

- Email
- SMS / Text
- Social media

Gain Access

- Dropper installs, or
- Exploit, or
- Victim clicks thru for install

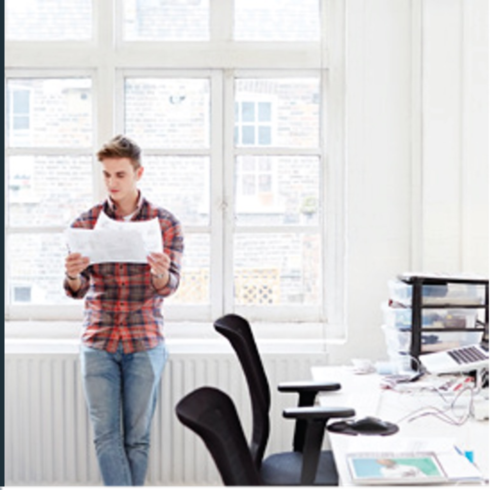
Elevate Privilege

- Install payload or
- Dropped apps, or
- Exploit vulns

Perform Espionage

Receive commands to:

- Send / exfiltrate private data, pictures, camera, audio



Lookout MPRA Mobile Phishing Risk Assessment

Get real mobile phishing statistics

What is MPRA ?

MPRA is a **M**obile **P**hishing **R**isk **A**ssessment platform used to demonstrate the need of protection against mobile phishing.

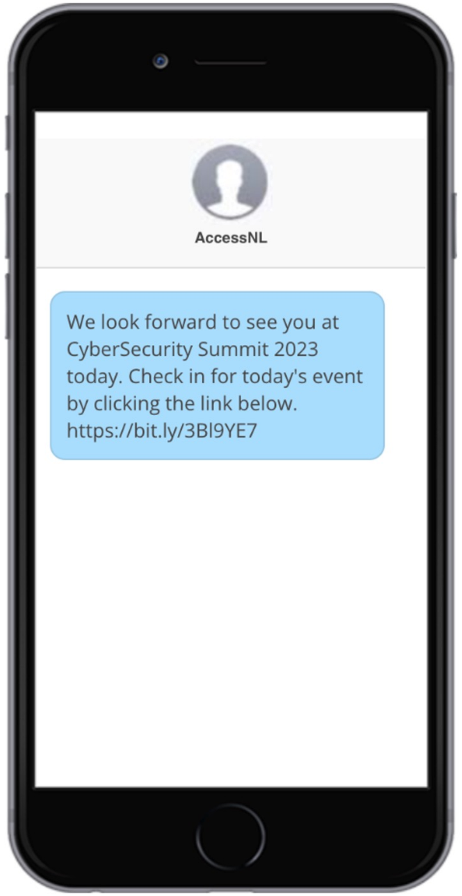
3 key business cases :

- **Before an event:** Send SMS messages to event attendees with an engaging scam content. Show analytics during the event reinforce a security-conscious mindset.
- **Mobile Phishing awareness:** Test customer/prospect employees by simulating mobile phishing via SMS. Evaluate their response and demonstrate the potential risks.
- **Demo purpose:** Send quick SMS during a demo using either your own phone number or your prospect's (always with their explicit consent).

MPRA can also be used with Lookout customers during cybersecurity-awareness campaign.

MPRA – Today's campaign statistics

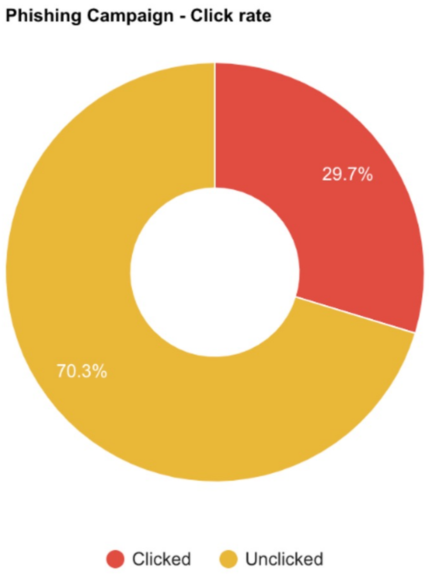
Message sent



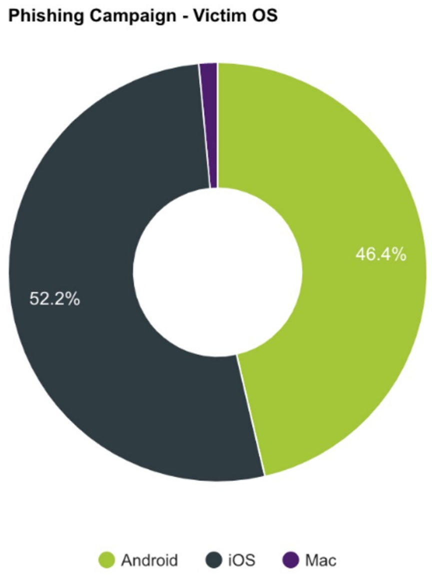
AccessNL

We look forward to see you at CyberSecurity Summit 2023 today. Check in for today's event by clicking the link below. https://bit.ly/3Bl9YE7

Statistics



Phishing Campaign - Click rate



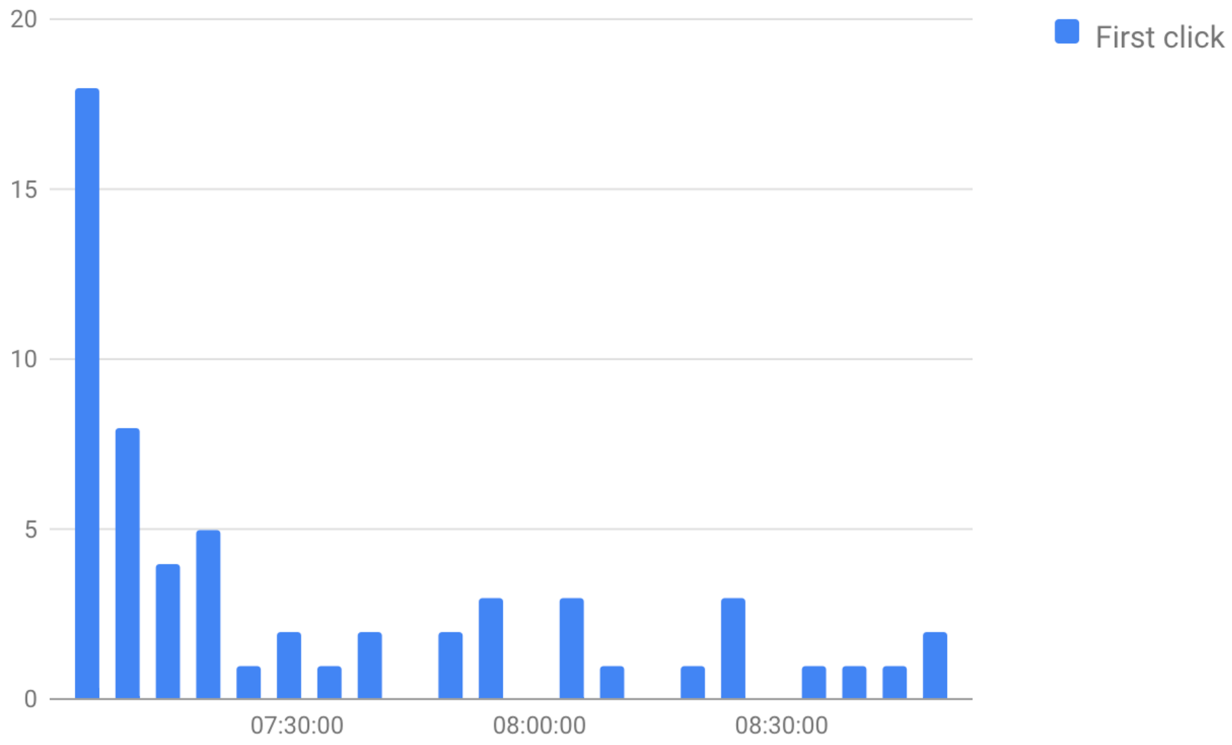
Phishing Campaign - Victim OS

Campaign metrics

Metric	Results
Number of SMS sent	245
Number of invalid or undelivered	6
Number of unique clicks	71 / 239
Click rate for this campaign	29.71 %
First click on	2023-06-15 06:01:01 (UTC +1)

Stats test

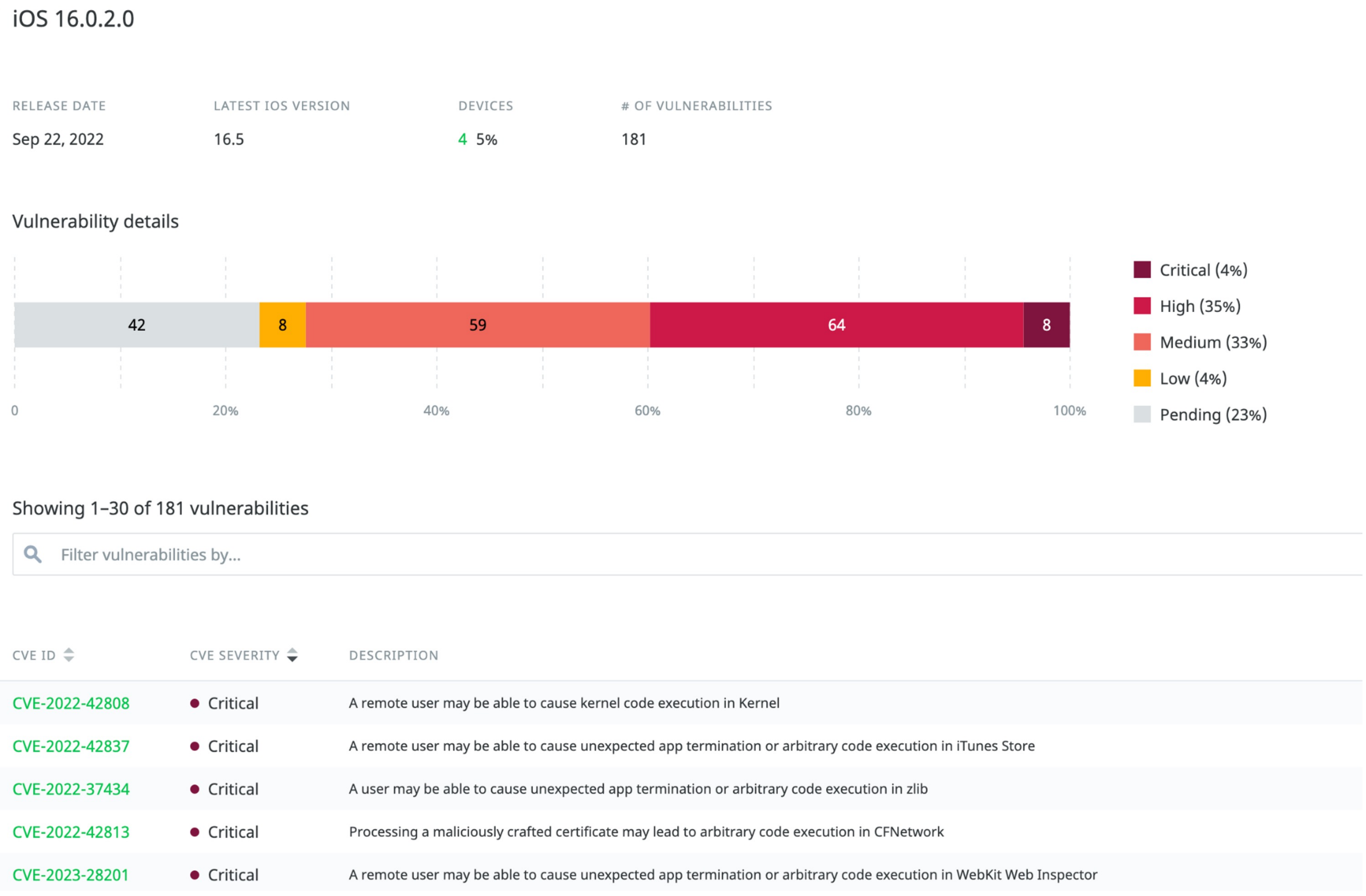
Number of clicks for the first 5 minutes interval



40% of all unique clicks (Devices) are running an outdated operating system that is vulnerable to remote exploits.

OS VERSIONS

Name	Version	Count
iOS	16.5	28
iOS	16.2	2
iOS	16.0.3	1
iOS	16.6	1
iOS	16.1	1
iOS	16.3.1	1
iOS	15.5	1
iOS	16.4.1	1
Android	13	12
Android	10	16
Android	12	4
macOS	Catalina 10.15	1
Unknown		1



iOS 16.0.2.0

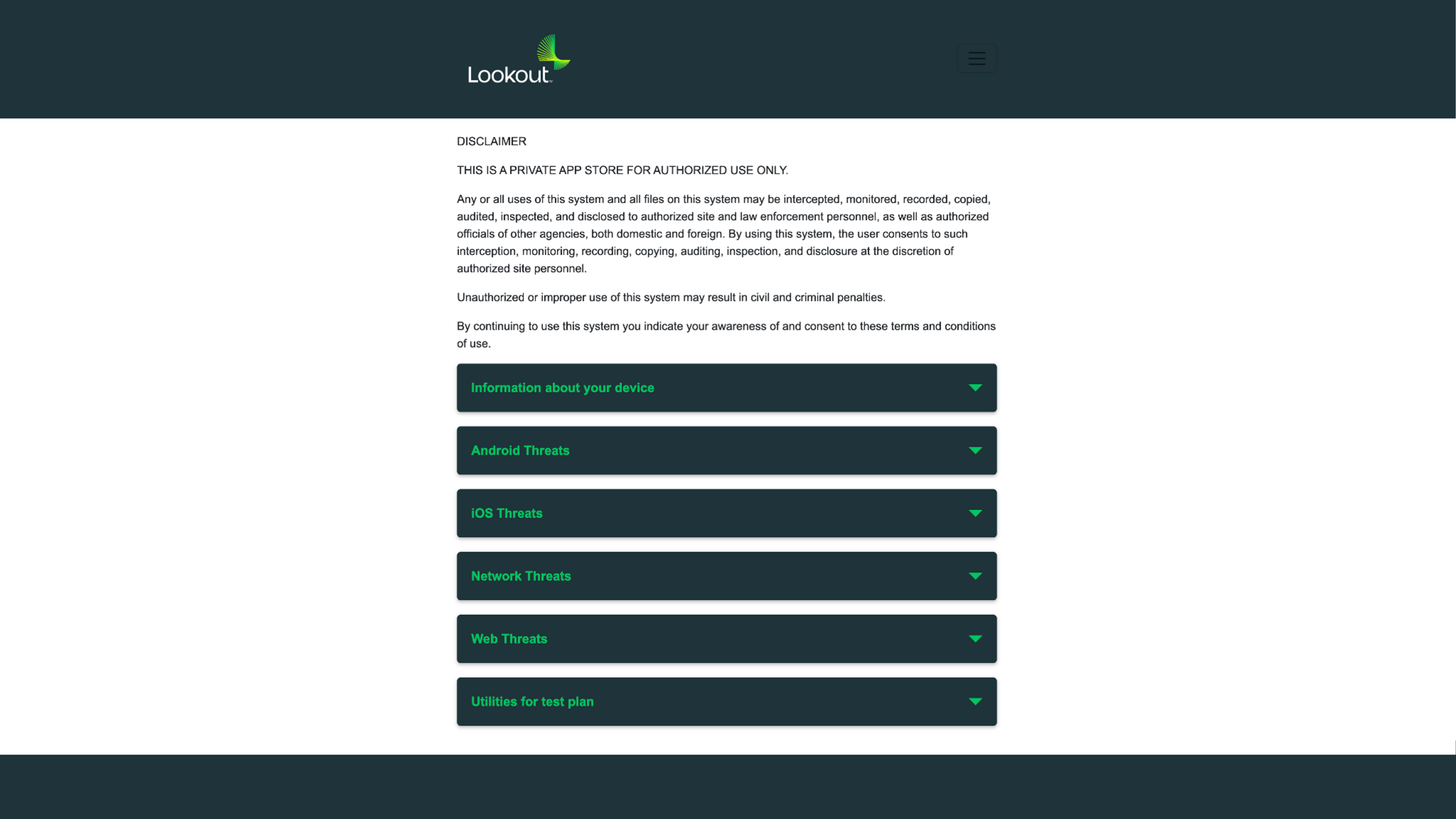
RELEASE DATE	LATEST IOS VERSION	DEVICES	# OF VULNERABILITIES
Sep 22, 2022	16.5	4 5%	181

Vulnerability details

Showing 1–30 of 181 vulnerabilities

Filter vulnerabilities by...

CVE ID	CVE SEVERITY	DESCRIPTION
CVE-2022-42808	● Critical	A remote user may be able to cause kernel code execution in Kernel
CVE-2022-42837	● Critical	A remote user may be able to cause unexpected app termination or arbitrary code execution in iTunes Store
CVE-2022-37434	● Critical	A user may be able to cause unexpected app termination or arbitrary code execution in zlib
CVE-2022-42813	● Critical	Processing a maliciously crafted certificate may lead to arbitrary code execution in CFNetwork
CVE-2023-28201	● Critical	A remote user may be able to cause unexpected app termination or arbitrary code execution in WebKit Web Inspector



DISCLAIMER

THIS IS A PRIVATE APP STORE FOR AUTHORIZED USE ONLY.

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site personnel.

Unauthorized or improper use of this system may result in civil and criminal penalties.

By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use.

Lookout™

You want to schedule your Mobile Phishing Risk Assessment?

Contact Ruth Lutterloch, Director GSI Alliances EMEA

ruth.lutterloch@lookout.com