Keep My Notes 1.80.147 - Improper Access Control

Summary

Affected versions	Version 1.80.147
State	Public
Release date	2022-06-01

Vulnerability

Kind	Improper Access Control
Rule	115. Security controls bypass or absence
Remote	No
CVSSv3 Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
CVSSv3 Base Score	6.1
Exploit available	Yes
CVE ID(s)	CVE-2022-1716

Proof of Concept

It is important to know that for a successful exploitation, the "Continue" button must be clicked repeatedly.

https://user-images.githubusercontent.com/51862990/168275718-5f8e230f-54f1-4c7c-8393-c58f0dcfda2b.mp4

Steps to reproduce

1. Install and configure frida as indicated in the following link.
2. Now just run this command to hook the `run` function so that it can be dynamically rewritten to bypass application protection.

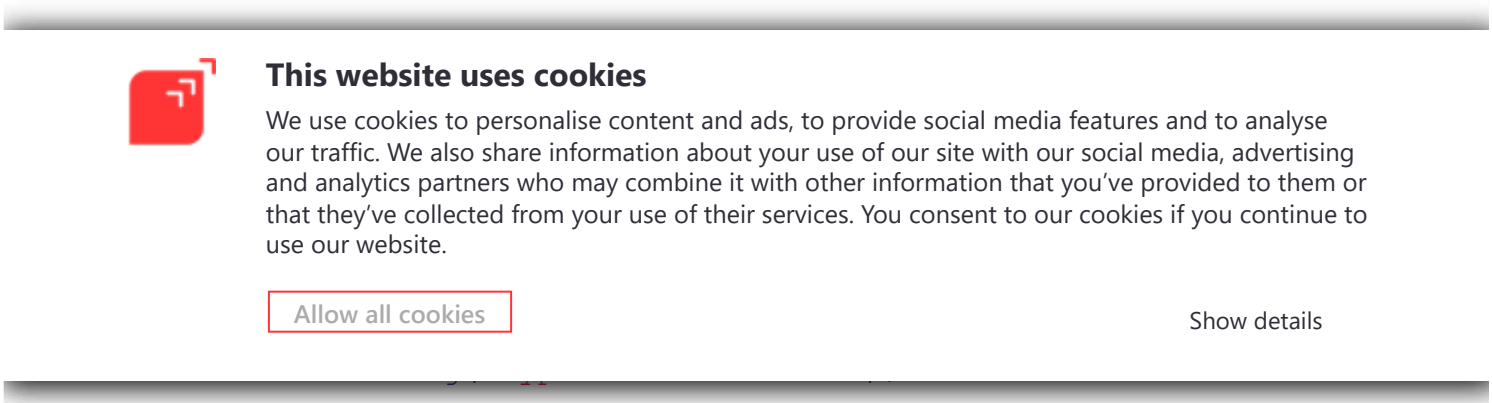
```
frida -U 'Keep My Notes' -l exploit.js
```

3. Now all you have to do is click the "Continue" button 3 or 4 times, then close the application and finally open it again.

System Information

- Package Name: org.whiteglow.keepmynotes
- Application Label: Keep My Notes
- Mobile app version: 1.80.147
- OS: Android 8.0 (API 26)

Exploit




```
            LockScreenActivity.$new().d();
        }
    })
```

Mitigation

There is currently no patch available for this vulnerability.

Credits

The vulnerability was discovered by Carlos Bello from the Offensive Team of `Fluid Attacks.`

References

Vendor page http://www.kitetech.co/keepmynotes

Timeline

- 2022-05-12
  Vulnerability discovered.
- 2022-05-12
  Vendor contacted.
- 2022-05-12
  Vendor Confirmed the vulnerability.

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Advisories

FAQ

Documentation

Contact