CyRC Vulnerability Advisory: CVE-2020-7958 biometric data disclosure vulnerability in OnePlus 7 Pro Android phone

Synopsys Cybersecurity Research Center
Posted by (https://www.synopsys.com/blogs/software-security/author/cyrc/) on Tuesday, April 14, 2020

Read the Synopsys Cybersecurity Research Center's (CyRC (https://www.synopsys.com/en-us/software-integrity/cybersecurity-research-center.html)) analysis of CVE-2020-7958, a biometric data disclosure vulnerability in the OnePlus 7 Pro Android phone.

(https://www.synopsys.com/blogs/software-security/wp-content/uploads/2019/04/cyrc-cybersecurity-research-center-header.jpg)

Overview

CVE-2020-7958 refers to a vulnerability that can lead to the disclosure of user biometric data in OnePlus 7 Pro Android phones. This vulnerability allows an attacker with root privileges to retrieve bitmap fingerprint images from the Trusted Execution Environment (TEE). Software builds prior to 10.0.3.GM21BA released on Jan. 7, 2020, are affected. Read the CVE entry. (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7958)

Impact

The vulnerability allows a privileged user (root) in the Rich Execution Environment (REE) to retrieve bitmap fingerprint images from the fingerprint sensor that should only be accessible in the TEE.

CVSS 3.0 vector:

```
AV:L/AC:H/PR:H/UI:R/S:C/C:H/I:N/A:N/E:F/RL:O/RC:C/CR:H/IR:X/AR:X/MAV:X/MAC:X/MPR:X/MUI:X/MS:X/MC:X/MI:X/MA:X
```

CVSS 3.0 overall score: 6.6

CWEs: CWE-215, CWE-489

Technical details

After the attacker obtains root privileges in the REE, it becomes possible to communicate directly with the factory testing APIs exposed by Trusted Applications (TAs) running in the TEE. The attacker can invoke a sequence of commands to obtain raw fingerprint images in the REE.

Remediation

Users should update the software build of their OnePlus 7 Pro devices to the latest available version. OnePlus Technology fixed this vulnerability in the 10.0.3.GM21BA software build (https://www.oneplus.com/uk/support/softwareupgrade/details?code=PM1574156267635).

Product description

OnePlus 7 Pro is a OnePlus flagship Android phone from 2019. More information about the device is available from the vendor's website (https://www.oneplus.com/uk/7pro#/).

Discovery credit

A team of researchers from the Synopsys Cybersecurity Research Center (https://www.synopsys.com/software-integrity/cybersecurity-research-center.html) (CyRC) in London discovered this issue:

- Georgi Boiko
- Artem Gonchar
- Andrew Lee-Thorp

Synopsys would like to thank the OnePlus security team for their swift and active engagement in addressing this vulnerability.

Timeline

- July 10, 2019: Synopsys consultants discover the issue.
- Aug. 14, 2019: Synopsys engages US-CERT.
- Oct. 7, 2019: Synopsys engages OnePlus.
- Nov. 13, 2019: Synopsys consultants test a vendor patch and confirm issue resolution.
- Jan. 7, 2020: OnePlus publishes the firmware update (https://www.oneplus.com/uk/support/softwareupgrade/details?code=PM1574156267635).
- April 14, 2020: CyRC publishes this advisory.

This post is filed under Security news and research (https://www.synopsys.com/blogs/software-security/category/security-research/).

Synopsys Cybersecurity Research Center

Posted by
Synopsys Cybersecurity Research Center

SEE AUTHOR ARCHIVE (https://www.synopsys.com/blogs/software-security/author/cyrc)

More from Security news and research

What is the cost of poor software quality in the U.S.? (https://www.synopsys.com/blogs/software-security/poor-software-quality-costs-us/)

Posted by Mike McGuire (https://www.synopsys.com/blogs/software-security/author/mmcguire/) on December 6, 2022

Software composition analysis (https://www.synopsys.com/blogs/software-security/tag/software-composition-analysis/)

CyRC Vulnerability Advisory: Remote code execution vulnerabilities in mouse and keyboard apps (https://www.synopsys.com/blogs/software-security/cyrc-advisory-remote-code-execution-vulnerabilities-mouse-keyboard-apps/)

Posted by Mohammed Alshehri (https://www.synopsys.com/blogs/software-security/author/alshehri/) on November 30, 2022

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

Beyond NVD data: Using Black Duck Security Advisories for version accuracy (https://www.synopsys.com/blogs/software-security/comparing-bdsa-with-nvd-version-accuracy/)

Posted by Lauren Fearon (https://www.synopsys.com/blogs/software-security/author/fearon/) on November 22, 2022

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

The “Software Vulnerability Snapshot” reports that 95% of tests uncovered vulnerabilities in target apps (https://www.synopsys.com/blogs/software-security/software-vulnerability-snapshot-report-findings/)

Posted by Fred Bals (https://www.synopsys.com/blogs/software-security/author/fbals/) on November 15, 2022

Dynamic application security testing (https://www.synopsys.com/blogs/software-security/tag/dast/)

Penetration testing (https://www.synopsys.com/blogs/software-security/tag/penetration-testing/)

Web application security (https://www.synopsys.com/blogs/software-security/tag/web-application-security/)

RELATED TAGS

Cybersecurity Research Center (https://www.synopsys.com/blogs/software-security/tag/cybersecurity-research-center/)

Software compliance, quality, and standards (https://www.synopsys.com/blogs/software-security/tag/software-quality-compliance/)

SEE ALL TAGS