Unpatched flaw in OnePlus phones lets rogue apps text messages - Again

Data: 2025-09-24 18:50:23

Autor: Inteligência Against Invaders

A vulnerability in multiple versions of OxygenOS, the Android-based operating system from OnePlus,

allows any installed app to access SMS data and metadata without requiring permission or user

interaction.

OnePlus, a subsidiary of Oppo, is a Shenzhen-based consumer electronics maker known for developing high-end smartphones at competitive pricing. While other major Chinese brands like Huawei and Xiaomi aren't available in the U.S., OnePlus devices are officially available in the country.

The flaw, tracked as CVE-2025-10184, and discovered by Rapid7 researchers, is currently unpatched and exploitable. The Chinese OEM failed to respond to Rapid7's disclosures to this day, and the cybersecurity company published the technical details along with a proof-of-concept (PoC) exploit.

Source of the problem

The problem arises from OnePlus changing the stock Android Telephony package to introduce additional exported content providers like PushMessageProvider, PushShopProvider, and ServiceNumberProvider.

The manifest for these providers does not declare a write permission for 'READ_SMS,' leaving it open to any app by default, even those that don't have SMS permissions.

[IMAGEM REMOVIDA]report.

So, while the read permission for SMS is correctly set, the write permission isn't, allowing the inference of SMS content when certain prerequisites are met:

1. Exposed table must already contain at least one row, so update() can return a non-zero "rows changed" result.
2. The provider must allow insert() so an attacker can create a dummy row to operate on if the table is empty.
3. The sms table must be in the same SQLite database file because the injected subquery must be able to reference it.

[IMAGEM REMOVIDA]

Device / Model

OnePlus 8T / KB2003

OnePlus 10 Pro 5G / NE2213

OnePlus 10 Pro 5G / NE2213

OnePlus 10 Pro 5G / NE2213

OnePlus 10 Pro 5G / NE2213

The researchers tried to contact OnePlus to share their findings on May 1 and followedup on alternative email addresses multiple times until August 16.

After receiving no response to seven separate communication attempts, the security firm publicly disclosed the details for CVE-2025-10184.

Shortly after publication of Rapid7’s report, OnePlus acknowledged the disclosure and said they have launched an investigation into the problem.

BleepingComputer has contacted OnePlus to request a comment, but we are still awaiting a response.

Until a patch is made available, it is recommended to keep the number of installed apps on your OnePlus device to a minimum, only trust reputable publishers, and switch from SMS-based two-factor authentication to OTP apps like Google Authenticator.

Since SMS isn’t properly isolated on OnePlus devices, sensitive communications should only occur on end-to-end encrypted apps.

Bill Toulas

Bill Toulas is a tech writer and infosec news reporter with over a decade of experience working on various online publications, covering open-source, Linux, malware, data breach incidents, and hacks.

You may also like: