Unpatched OnePlus vuln allows rogue app SMS access - InfoSecBulletin -

Data: 2025-09-25 18:59:54

Autor: Inteligência Against Invaders

A ***flaw*** in various versions of OnePlus's OxygenOS lets any app access SMS data and metadata without needing permission or user consent.

OnePlus is a Shenzhen-based tech company recognized for producing high-quality smartphones at affordable prices. Unlike other major Chinese brands like Huawei and Xiaomi, OnePlus phones are officially sold in the U.S.

The vulnerability named CVE-2025-10184, found by Rapid7, remains unpatched and exploitable. The Chinese OEM has not responded to Rapid7's reports, prompting the cybersecurity firm to share technical details and a proof-of-concept (PoC) exploit.

Source of the problem:

The ***issue*** comes from OnePlus modifying the stock Android Telephony package to add new 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.

Client inputs aren't sanitized, which allows "blind SQL injection" to potentially reconstruct SMS content from the device database by brute-forcing it one character at a time.

"By using an algorithm to repeat this process for each character in each row returned by the sub query, it's possible to exfiltrate the database content, using the return value from the update method as an indicator of true/false," describes Rapid7 in the report.

The SMS read permission is correctly set, but the write permission is not, which allows for inferring SMS content under certain conditions:

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

Impact and response:

The issue affects all versions of OxygenOS, from 12 to the latest, 15, built on Android 15.

Rapid7 researchers have confirmed a vulnerability in OnePlus 8T and 10 Pro devices using different versions of OxygenOS and Telephony packages, but their findings are likely not comprehensive.

“While the build numbers above [on the table] are specific to the test devices, as the issue affects a core component of Android, we expect this vulnerability to affect other OnePlus devices running the above versions of OxygenOS, i.e., it does not seem to be a hardware-specific issue,” explained Rapid7.