

PRESS RELEASE

Technical security analysis of the "Temu" mobile app

Unusual technical anomalies in the Temu app – caution is advised

Zug, December 5, 2024 – The Temu app exhibits technical abnormalities such as dynamic loading of code and additional encryption layers that make it difficult to reach a final assessment. However, there are no critical security risks or solid evidence of illicit surveillance.

Temu, a popular e-commerce app from China, is enjoying growing popularity in Switzerland. At the same time, there is an increasing focus on the cybersecurity risks of such apps. The National Test Institute for Cybersecurity NTC has carried out an independent security analysis of the Temu app in order to assess the actual risks for users.

Unusual technical anomalies

The analysis identified a number of "red flags":

- **Dynamic loading of code in proprietary runtime environment:** This allows the app to change its behavior on the fly. Developers can adapt features and content flexibly with no need for app store updates, i.e. without the need for initiation or approval by the user.
- **Additional encryption layers:** Although these layers can increase the protection of data, they can also potentially be used to conceal unwanted data transfers.

Although these characteristics are not necessarily malicious, they present challenges when it comes to making a complete assessment.

Other security risks are mostly harmless

Otherwise, the analysis shows that the Temu app contains no obviously critical security risks or evidence of illicit surveillance. The app's permissions and behavior largely meet the standards of e-commerce applications. Compared with similar apps, Temu requires fewer and less-problematic permissions.

NTC recommendations

While the analysis did not find any concrete evidence of malicious activities, the NTC recommends critically questioning the use of the Temu app, particularly in business and government contexts – as is the case for any apps with wide-ranging permissions. Users should take the following precautions:

- Minimize permissions granted to the app.
- Ensure regular updates of the operating system.
- Consider using the service via a mobile browser instead to reduce the attack surface.

About Temu and cybersecurity concerns

The app is operated by the Chinese company PDD Holdings Inc. and is subject to Chinese law, which is considered inadequate in terms of data protection from a European perspective. Companies and authorities should take this into account when using the app.

Independent analysis

The analysis was carried out independently by the NTC with no external influences. The findings focus exclusively on cybersecurity aspects and deliberately refrain from evaluating other controversial topics such as business practices or product quality.

[To the security analysis](#)

Media contact:

Andreas W. Kaelin, Executive Management
+41 41 210 11 03, andreas.kaelin@ntc.swiss

About the National Test Institute for Cybersecurity NTC

The National Test Institute for Cybersecurity NTC contributes to Switzerland's security and digital sovereignty by proactively identifying critical vulnerabilities and supporting their removal. As a not-for-profit association based in Zug, the NTC observes the principles of independence and objectivity. It conducts cybersecurity testing of networked infrastructures, devices and applications that are of great importance to society and the economy. <https://en.ntc.swiss/>