Browser Extensions Security Check Report

Objective: Identify and remove potentially harmful browser extensions.

Tools Used: Google Chrome

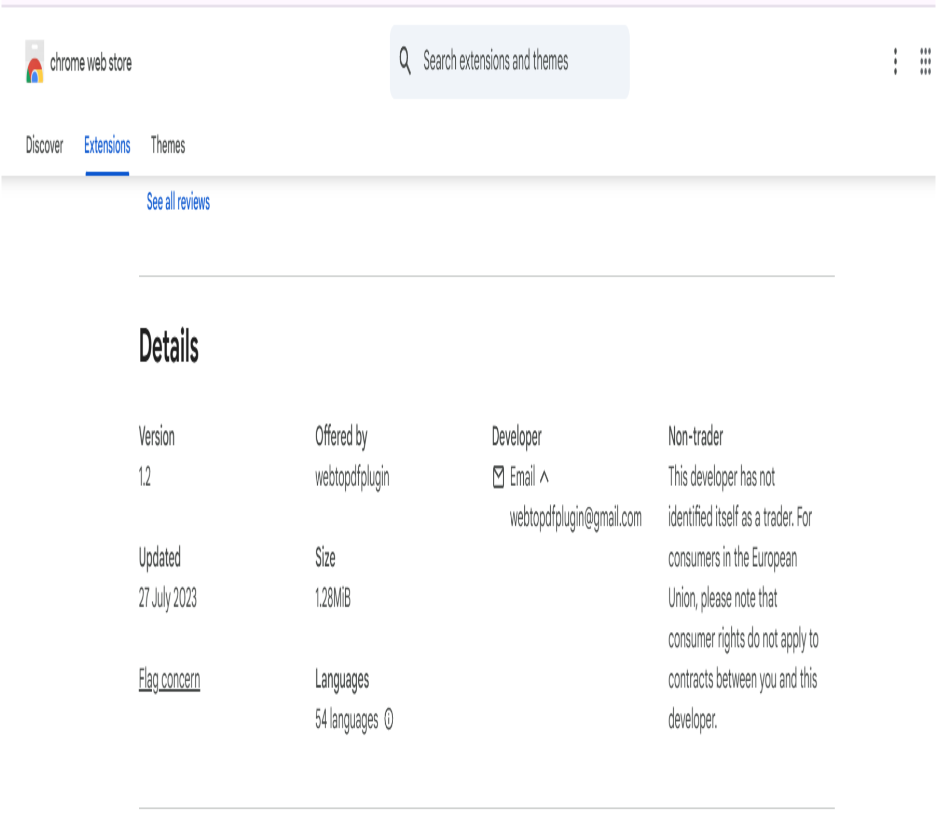
1. Opened Chrome Extensions Manager (chrome://extensions/).
2. Reviewed all installed extensions and checked their permissions.
3. Researched any unfamiliar extensions online.
4. Identified suspicious extension based on permissions, developer information, and reviews.
5. Removed suspicious extension and restarted browser.
6. Verified browser performance and security post-removal.

Safe Extension Example:

Extension Name: Grammarly
Reason: Well-known developer, transparent privacy policy, widely used with positive reviews.

Suspicious Extension Example:

Extension Name: webtopdfplugin
Reason: Unknown developer, generic Gmail contact, broad permissions (read/change data on all sites), minimal transparency, low trust factor.



Details

Version
1.2

Offered by
webtopdfplugin

Developer
Email
webtopdfplugin@gmail.com

Non-trader
This developer has not identified itself as a trader. For consumers in the European Union, please note that consumer rights do not apply to contracts between you and this developer.

Updated
27 July 2023

Size
1.28MiB

Flag concern

Languages
54 languages

Risks of Malicious Extensions:

- Stealing sensitive data such as passwords and credit card numbers.
- Tracking browsing history for targeted ads or malicious purposes.
- Injecting malicious scripts into webpages.
- Redirecting users to phishing or scam sites.
- Displaying unwanted ads or pop-ups.

Recommendations:

- Install extensions only from trusted developers.
- Review permissions before installation.
- Keep browser and extensions updated.
- Remove extensions that are unused or suspicious.
- Regularly audit installed extensions.

Conclusion: The suspicious extension 'webtopdfplugin' was identified and removed to improve browser security and performance.