Microsoft Edge to block malicious sideloaded extensions

Data: 2025-09-26 16:37:32

Autor: Inteligência Against Invaders

Microsoft is planning to introduce a new Edge security feature that will protect users against

malicious extensions sideloaded into the web browser.

Edge enables developers to install extensions locally (also known as sideloading) for testing purposes before publishing them to the Microsoft Edge Add-ons store by toggling the “Developer Mode” option on the Extensions management page and clicking the “Load unpacked” button.

However, users can also sideload third-party extensions that aren’t distributed through official channels and aren’t scanned for malware.

While users can remove dangerous extensions via the Extensions management tab by clicking the “Remove” link in the extension card, it’s usually too late if threat actors have tricked the user into installing them, as shown by attacks that have affected hundreds of thousands of users in recent years and can also force-install malicious extensions hosted on official add-on stores.

However, as Redmond revealed on Thursday in the Microsoft 365 roadmap, “Microsoft Edge will detect and revoke malicious sideloaded extensions.”

Although the company didn’t provide further details on how these dangerous extensions will be identified, the new security feature is set to launch in November for standard multi-tenant instances worldwide.

In recent months, Microsoft has updated the “Publish API for Edge extension developers” to enhance security for developer accounts and the browser extension update process. It has also started testing a new feature designed to warn users of extensions that negatively affect Edge’s performance.

In February, it also introduced an AI-powered scareware blocker for the Edge web browser, which utilizes machine learning (ML) to detect tech support scams by detecting signs of scareware scams in real-time using a local machine learning model.

This month, Microsoft began rolling out HTTPS-First Mode in Microsoft Edge, which automatically upgrades HTTP connections to HTTPS when possible. Additionally, starting with Edge v140 (released in August), the web browser will automatically discard sleeping tabs to save memory.

[IMAGEM REMOVIDA]