UXSS bug on Microsoft Edge allows hackers to steal user information

Last week, Microsoft rolled out updates to its Edge browser to fix two security flaws, including a UXSS vulnerability that could be exploited to inject and execute arbitrary code in the content of any web page. which.

The vulnerability, codenamed CVE-2021-34506 (CVSS score: 5.4), stems from a UXSS issue. It is activated when automatically translating web pages using pre-installed features through Microsoft Translator.

"Unlike normal XSS attack, UXSS is an attack type where vulnerabilities reside inside the browser or browser extension to create conditions similar to XSS conditions and execute malicious code. " - The Hacker News quotes CyberXplore experts. "When such vulnerabilities are found and exploited, browser behavior is affected and security features may be ignored or disabled."

Specifically, the researchers discovered that the translation feature contained a vulnerable piece of code that failed to clean the input. As a result, an attacker has the ability to insert malicious JavaScript code anywhere in the website. The malicious code is then executed when the user clicks on the address bar prompt to translate the page.

As a method of POC exploit, the attack is easily accomplished simply by adding non-English comments to a YouTube video, along with the XSS payload.

Likewise, the XSS payload and a Facebook friend request whose profile contains other language content were found to execute code immediately after the requester's friend checked the friend's profile. friend.

On June 24, 3 weeks after receiving the report, Microsoft fixed the problem and awarded $20,000 to CyberXplore security experts.

You can download the latest update (version 91.0.864.59) for the Chromium-based browser by going to **Settings and more -> About Microsoft Edge (edge://settings/help)** .

You finished reading the article "**UXSS bug on Microsoft Edge allows hackers to steal user information**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
