Microsoft Edge Flaw Lets Hackers Steal Local Files, MS still full of hacker back doors

By **Catalin Cimpanu**

0

Microsoft has fixed a vulnerability in the Edge browser that could be abused against older versions to steal local files from a user's computer.

The good news is that social engineering is involved in exploiting the flaw, meaning the attack cannot be automated at scale, and, hence, present a smaller level of danger to end users.

Edge flaw is SOP-related

Discovered by Netsparker security researcher Ziyahan Albeniz, the vulnerability involves the Same-Origin Policy (SOP) security feature that all browser support.

In Edge, and all other browsers, SOP works by preventing an attacker from loading malicious code via a link that does not matches the same domain (subdomain), port, and protocol.

Albeniz says that Edge's SOP implementation works as intended except one case —when users are tricked into downloading a malicious HTML file on their PC and then running it.

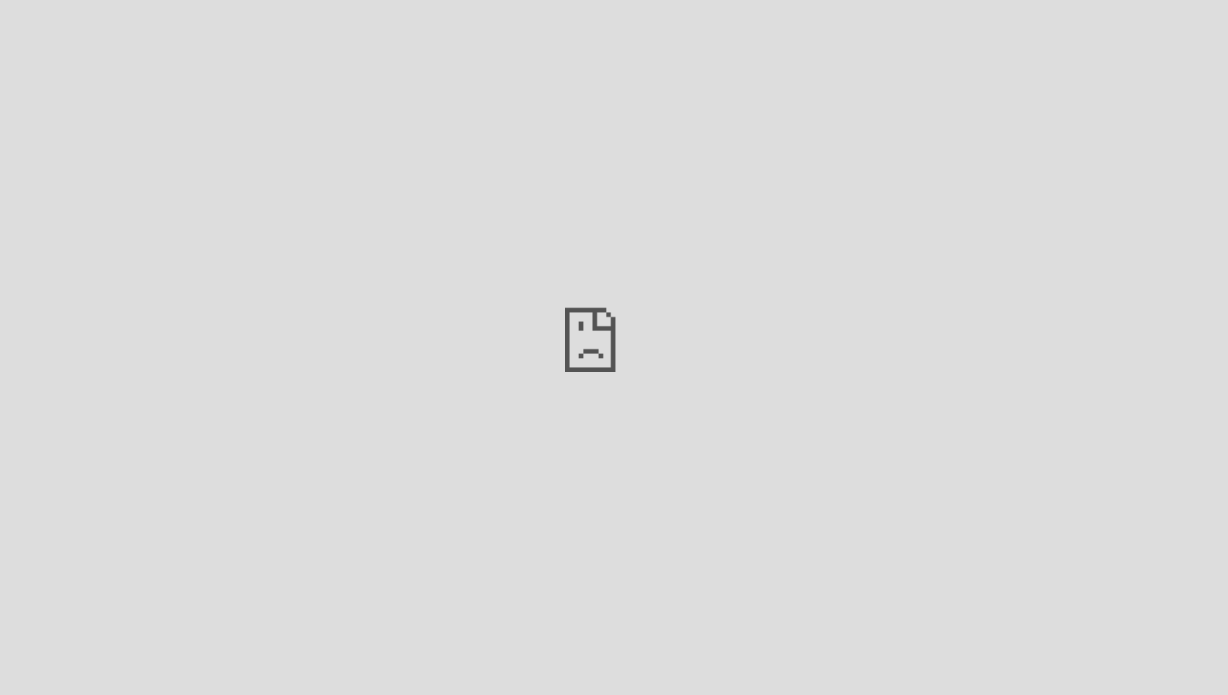
When the user runs this HTML file, its malicious code will be loaded via the file:// protocol, and because it's a local file, it will not have a domain and port value.

What this means is that this malicious HTML file can contain code that collects and steals any data from local files accessible via a "file://" URL.

Because any OS file can be accessed via a file:// URL inside a browser, this essentially gives the attacker free reign to collect and steal any local file he wants.

Flaw useful in targeted attacks

Albeniz says that during tests he was able to steal data from local computers and send it to a remote server by executing this file in both Edge and the Mail and Calendar app. He also recorded a video of the attack, embedded below.



The attack requires an attacker knowing where various files are stored, but some OS and app config and storage files are in most cases stored at the same location on the vast majority of devices. Furthermore, the location of some files can be inferred or guessed.

The vulnerability may not be useful in the case of en-masse malware distribution campaigns, but it could be useful in more targeted attacks on high-value targets.

Warning for opening HTML files of unknown origin

But while Microsoft has addressed this issue in recent Edge and Mail and Calendar app versions, Albeniz now wants to warn users about the dangers of running HTML files they receive from strange persons or via email.

The researcher's warning is valid because HTML files are not usually associated with regular malware distribution campaigns.

According to an F-Secure report, just five file types make up 85% of all malicious attachments sent via email spam campaigns. They are ZIP, DOC, XLS, PDF, and 7Z.

"The only way to protect yourself is to update to the latest versions of the Edge browser and Windows Mail and Calendar applications. And, of course it's best to never open attachments from unknown senders, even if the extension doesn't initially appear to be malicious," the researcher said in a report he published yesterday, entitled "Exploiting a Microsoft Edge Vulnerability to Steal Files."

Albeniz said other browsers were not vulnerable to the SOP vulnerability he reported to Microsoft. The researcher also told Bleeping Computer that the Redmond-based OS maker fixed the vulnerability (CVE-2018-0871) with the release of the June 2018 Patch Tuesday.

Related Articles:

Microsoft Edge's XSS Filter Appears to Be Broken

Microsoft Edge Bug Exposes Content From Other Sites via HTML5 Audio Tag