

Home (<https://www.bleepingcomputer.com/>) > News (<https://www.bleepingcomputer.com/news/>)
> Security (<https://www.bleepingcomputer.com/news/security/>)
> Screencastify Chrome extension flaws allow webcam hijacks

Screencastify Chrome extension flaws allow webcam hijacks

By **Bill Toulas** (<https://www.bleepingcomputer.com/author/bill-toulas/>)
May 24, 2022 12:45 PM 0



The popular Screencastify Chrome extension has fixed a vulnerability that allowed malicious sites to hijack users' webcams and steal recorded videos. However, security flaws still exist that could be exploited by unscrupulous insiders.



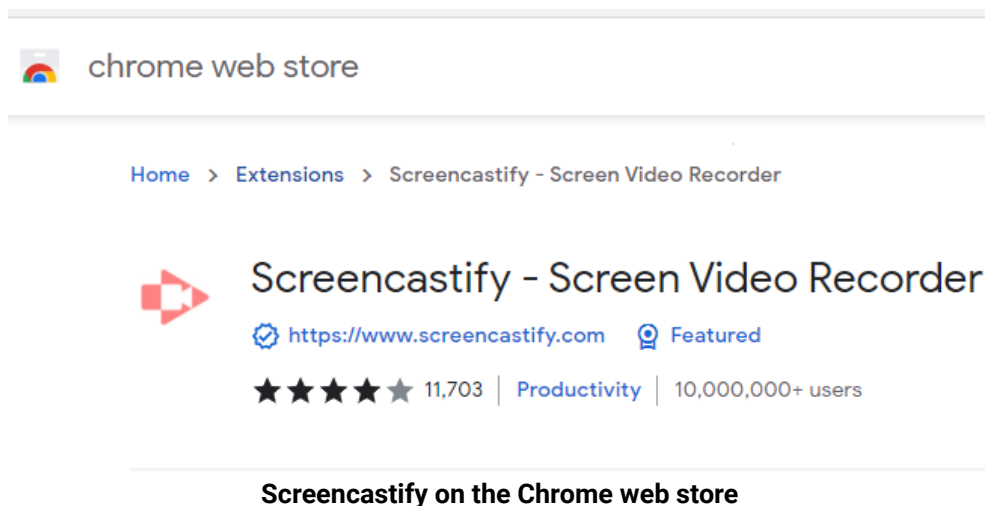
The vendor acknowledged the cross-site scripting (XSS) vulnerability and promptly fixed it after security researcher Wladimir Palant reported it responsibly on February 14, 2022.

However, the same privacy and security-related risks remain unaddressed, keeping users at potential risk from websites that partner with the Screencastify platform.

Palant decided to publish a write-up on his blog to warn the millions of people who use Screencastify of the underlying risks, as the vendor has not fully fixed the issues after three months.

A convenient video tool

Screencastify is a screen recorder, video editor, and media sharing browser extension with over 10,000,000 installs on the Chrome web store.



The number of installations may be much higher, as the ten million is the maximum download figure supported by the platform.

The tool's popularity exploded during the pandemic, as it's an easy-to-use and powerful utility that can prove helpful in a range of everyday tasks.

The extension is integrated with the vendor's website, which is necessary for offering video editing functionality. Unfortunately, while this is convenient and straightforward, it is also a source of risks.

Google Drive and API access

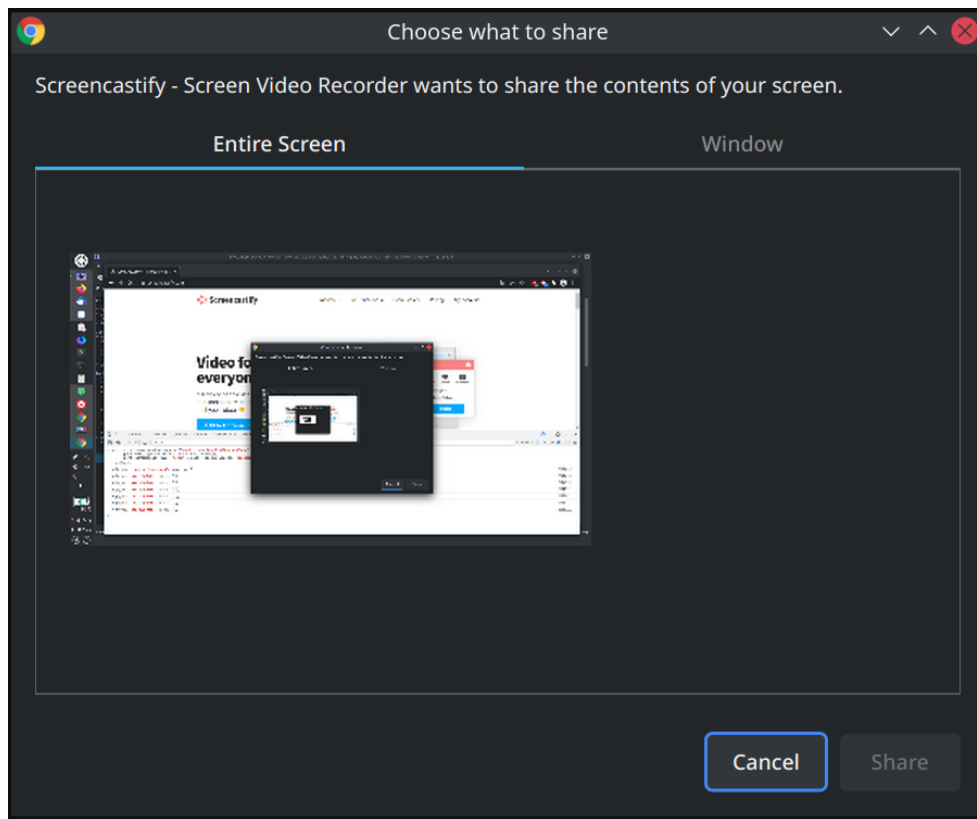
The first issue arises from Screencastify's request to access the user's Google Drive and create a permanent Google OAuth access token to their accounts.

This access token is required to create a visible (not hidden) folder that hosts the user's video projects, which are uploaded or downloaded using the service without requiring additional user actions.



The platform also requests permissions to access WebRTC API once, so access to the capturing functions is enabled from the user's first recording attempt.

Permissions for accessing Chrome's desktopCapture API and tabCapture API are granted automatically upon the installation of the extension.



Requesting recording API access on Chrome (*palant.info*)

Silent webcam launch

An XSS vulnerability existing in the website allowed attackers to enable Screencastify to record a video, which would be uploaded to Google Drive. This same vulnerability allowed the stealing of the Google Drive OAuth token, which the threat actors could then use to download the created video, and anything else stored on Google Drive.

To make matters worse, the researcher developed a PoC exploit attackers could use to launch the webcam of users of the Screencastify extension without indicating the action.

"The problem was located in the error page displayed if you already submitted a video to a challenge and were trying to submit another one," explains Palant in his blog post (<https://palant.info/2022/05/23/hijacking-webcams-with-screencastify/>)

"This error page is located under a fixed address, so it can be opened directly rather than triggering the error condition."



The exploitable error page (*palant.info*)

Since there's no validation taking place here, if the attacker sends this link to a target and tricks them into clicking the "View on Classroom" button, they could achieve an XSS condition.

The researcher developed a clickjacking attack by creating a concept page that loaded the vulnerable error page in an invisible frame and positioning the button under the victim's cursor.

Once the user clicks the mouse, which is the only action required for the exploit to work, Screencastify retrieves the Google access token, making video recording or Drive access possible for the attacker.

Problems still exist

While Screencastify fixed the XSS vulnerability that allowed any malicious site to hijack webcams, problems still exist that could allow an employee or compromised site to silently record videos from Screencastify user's devices.

According to Palant, Screencastify's domain serves multiple applications from various companies that use the project, which opens up a large XSS attack surface.



These companies are Webflow, Teachable, Atlassian, Netlify, Marketo, and ZenDesk, all of which control subdomains with no real protection in terms of content security.

- Webflow: www.screencastify.com
- Teachable: course.screencastify.com
- Atlassian: status.screencastify.com
- Netlifyrunning: quote.screencastify.com
- Marketo: go.screencastify.com
- ZenDesk: learn.screencastify.com

According to the analyst, Screencastify's latest version, 2.69.0.4425, is still vulnerable to unauthorized API and Google OAuth token access, and the handler to start video recording is still present.

"Not much appears to have changed here, and I could verify that it is still possible to start a webcam recording without any visual clues." says the researcher.

The vendor told Palant they plan to add a strict content security policy, but this has not happened yet, so users are still at risk.

Even if XSS flaws were to be addressed by all of the companies that use Screencastify, the question of trust towards these entities remains, as choosing to use the extension is entrusting third parties with full access to your Google Drive contents.

All that it would take is for these sites to be modified by a rogue employee or by a hacker who compromises a site to, once again, record videos from Screencastify users' webcams.

BleepingComputer has contacted Screencastify regarding the remaining issues but has not received a reply at this time.

-The above article was updated on May 24 after receiving clarifications from the researcher

