



0, 2020

PRIVILEGE ESCALATION VULNERABILITY IN SPLASHTOP STREAMER



powered by:
[Cookie Information \(https://cookieinformation.com/\)](https://cookieinformation.com/)

You control your data

We and our business partners use technologies, including cookies, to collect information about you for various purposes, including:

Anders Kusk (/tech-blog?author=5e21c687c8ae141b3ef5aa77)

1. Functional
2. Statistical
3. Marketing

This blog post highlights bugs found in installed software while doing vulnerability research. The process for this publication is aligned with the Improsec Responsible Disclosure Policy. By clicking 'Accept', you give your consent for all these purposes. You can also choose to specify the purposes you consent to by ticking the checkbox next to the purpose and clicking 'Save settings'.

CVE registered

withdraw your consent at any time by clicking the small icon at the bottom left corner of the website.

- CVE: CVE-2020-12431 (<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12431>)
You can read more about how we use cookies and other technologies and how we collect and process personal data by clicking the link. [Read more about cookies](#)

What is Splashtop Streamer

Splashtop Streamer is a remote desktop application that allows users to share their desktop and remotely control workstations. The affected component is the Splashtop Updater that is bundled with the Splashtop Streamer, as well as certain other Splashtop products.

Strictly necessary Functional Statistical Marketing

Timeline

- 13/2-2020 – Improsec identified the vulnerability.
- 21/2-2020 – Contact to Splashtop reached, a vulnerability disclosed to the software vendor.
- 24/2-2020 – The software vendor acknowledged the vulnerability report.
- 13/3-2020 – Software vendor releases an internal software update for testing.
- 19/3-2020 – Improsec reviewed the update and acknowledge that the vulnerability was fixed.
- 6/4-2020 – Improsec contacts vendor again about another vulnerability in the same update function.
- 7/4-2020 – The software vendor acknowledged the vulnerability report.
- 14/4-2020 – Software vendor releases an internal software update for testing.
- 15/4-2020 – Improsec reviewed the update and acknowledge that the vulnerability was fixed.
- 25/4-2020 – Software vendor releases patched software packages.
- 19/5-2020 – Public disclosure of the vulnerability.

We want to thank Splashtop Inc. for an effective and professional response.