0, 2020

PRIVILEGE ESCALATION VULNERABILITY IN SPLASHTOP STREAMER

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

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.

CVE registered

- CVE: CVE-2020-12431 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12431)

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 Splashtop Streamer, as well as certain other Splashtop products.

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.