May 27, 2020

How not to handle responsible disclosure - SmartDraw 2020

Jacob Petersen (/tech-blog?author=5ea94dbc9ef5123f214bbceb)

Dealing with responsible disclosure can be a time-consuming process for both parts, and can especially become a tedious task, if the software vendor in question, either ignores the inquiries or becomes hostile. Occasionally we still see software vendors pursue and threaten researchers who contact them about a security vulnerability in their product. They might insist that it's not worth their time to fix the issue or even threaten with lawsuits, if we release our findings.

Just recently we had such an experience, wherein the software vendor unfortunately chose to first ignore our inquiry, only to attempt to fix the issues we found silently without informing us.

Responsible disclosure isn't about exposing organizations for making bad or unsecure software. It's about helping them make better software. When an organization receives a responsible disclosure inquiry about vulnerability in their software, they have nothing to lose. Many security enthusiasts like myself do it as a hobby, because we find it fun and interesting and a by-product of that, is helping organizations keep their software secure, free of charge. Going on the defence will only make other security enthusiasts less inclined to look for vulnerabilities in that particular company's software, potentially leaving critical vulnerabilities unnoticed, which could be found and exploited by malicious actors.

To avoid these scenarios, software vendors should have a responsible disclosure policy that states what types of vulnerabilities they would like to be informed about, the format of the inquiry and most importantly how to contact them, should you wish to send a responsible disclosure inquiry.

Responsible disclosure - SmartDraw 2020

CVE registered

- CVE: CVE-2020-13386 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13386)

On May 3rd I discovered that the SmartDraw 2020 software product by SmartDraw, LLC, is installed using weak folder permissions, giving low privileged users inherited write permissions on the installation path of the product. The product is installed under "C:\SmartDraw 2020" and the group "Authenticated Users" has written permissions on the folder, as seen below.