Disclaimer

This is a report concerning studentKeeper web filtering software. This is not a tutorial on bypassing school internet, nor is this a recommendation that you do so.
Domains, instructions, and data relating to the vulnerability have been redacted for the protection of both the vendor (ativion) and school districts. Do not contact adison for instructions on how to “bypass your student internet”, you will be blocked from ever sending another email. Contact information will be provided for questions, comments, and concerns about the vulnerability.

Author

Name: Adison Verlice
Email: averlicetech@proton.me
For encrypted email, use this PGP public key
For key verification, go here.

Vendor information

Vender: Ativion
Product; StudentKeeper
Website: https://www.ativion.com/studentkeeper/
Description (taken directly from ativion))
“StudentKeeper, powered by ContentKeeper, is a comprehensive platform that combines (enterprise-level) web filtering, classroom management, and student well-being tools.“

Vulnerability information

Vulnerability info: failOpen policy

The vulnerability in question relies on a DNS network hijack to work, but more on this later.
The StudentKeeper agent has a heartbeat in order to do “just in time” filtering, where it must contact this domain every time a request is made to visit a website or contact a domain. The domain is redacted. Rather than failing closed, where the filter would have let nothing through, it failed open, meaning that any request, regardless of if it cannot contact its domain or “phone home”, will go through.

How this vulnerability was tested

The vulnerability was tested by mapping this domain to 0.0.0.0 using a custom DNS setup, though this can work on commercial DNS servers where the domains of those servers are not blocked (E.G. nextDNS, openDNS, quad9).

How the user exploits the vulnerability

1. The user must find a way to actively block connections to the callback domain.
2. The user must flush the web socket pools in the browser, and/or restart the computer.

Risk

This could set a precedent where it violates the children's internet protection act (CIPA), exposes kids to pornographic/harmful contact, and also disables logging for the administrator.

Solutions to this problem

1. Network side filtering: rather than using a client which most of the time relies on the browser's skin (server name indication) use a pac proxy and/or VPN back to your schools and/or educational institutions network with filtering enabled. This ensures there is a central point of contact, and that it cuts off the connection if it cannot contact the proxy.
2. Enforce DNS: you can attempt to enforce your own DNS servers, though this solution will not work if the students network has DPI which blocks the source domain.
3. (for ativion) fail closed policy: change the code where it fails closed if it cannot “phone home”.