
 **mame82 / munifying-web**


Watch 1


★ Star 19

Fork 2

<> Code

 Pull requests 0

 Security

 Insights


Join GitHub today


Dismiss


GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.


Sign up


No description, website, or topics provided.


 4 commits

 1 branch

 0 packages

 0 releases

 1 contributor






 GPL-3.0


Branch: master ▾

New pull request

Find file

Clone or download ▾

 mame82 Text	✓ Latest commit 0419d85 21 hours ago
 LICENSE	text 21 hours ago
 README.md	Text 21 hours ago
 index.html	text 21 hours ago
 main.js	text 21 hours ago

 README.md

munifying-web

Experimental in-browser implementation of CVE-2019-13054/CVE-2019-13054 from Chrome 78+.

The page utilizes the new WebHID API to extract AES encryption keys from vulnerable dongles.

As this is a PoC, there is no proper error handling implemented. The code is supposed to work with Logitech receivers utilizing a Texas Instruments Chip (R500, SPOTLIGHT, LightSpeed Logitech Unifying with RQR24.x). The vulnerability was patched with firmware RQR24.10 / RQR24.11 for Logitech Unifying receivers.

How to use

Browse to <https://mame82.github.io/munifying-web/> with Chrome 78+. Once the 'Experimental Web Platform features' are enabled, the `dump` button should present a dialog, which let you choose from connected Logitech receivers. If the dongle is vulnerable, extracted keys will be printed to the page.

Everything runs locally in the browser.

Inspect the `main.js` file to adopt this for other projects.

For a full implemetation of a dumping/flashing tool for Unifying receivers, watch out for [munifying](#)

DISCLAIMER

this code is a Proof of Concept and should be used for authorized testing and/or educational purposes only. The only exception is using it against devices owned by yourself.

I take no responsibility for the abuse of this code or any information given in the related documents.

I DO NOT GRANT PERMISSIONS TO USE this code TO BREAK THE LAW.

I disclaim any warranty for this code, it is provided "as is".