main Go to file Code

bikini Add FFmpeg RASC DLTA calc PoC d7bdd1d · 14 hours ago

7zip-rar5-motw-chai...	Add exploitarium arch...	4 days ago
anydesk-printer-com...	Add exploitarium arch...	4 days ago
c-ares-tcp-uaf-calc-poc	Add live SSH transport...	yesterday
docker-cp-copyout-d...	Add exploitarium arch...	4 days ago
ffmpeg-rasc-dlta-cal...	Add FFmpeg RASC DL...	14 hours ago
firefox-smartwindow...	Remove Smart Windo...	3 days ago
floci-apigateway-vtl-r...	Add Floci IAM scope b...	3 days ago
flowise-mcp-env-cas...	Add exploitarium arch...	4 days ago
ghidra-12.1.2-rce-ac...	Add exploitarium arch...	4 days ago
gitea-act-runner-con...	Add exploitarium arch...	4 days ago
imagemagick-gs-del...	Add exploitarium arch...	4 days ago
libssh2-cve-2026-552...	Update README.md	4 days ago
libssh2-publickey-list...	Add live SSH transport...	yesterday
lunar-modrinth-chai...	Add exploitarium arch...	4 days ago
mybb-limited-acp-to-...	Add exploitarium arch...	4 days ago
nghttp2-nghttpx-up...	Add nghttp2 nghttpx ...	20 hours ago
nmap-ipv6-extlen-wr...	Add Nmap IPv6 exten...	4 days ago
objdump-dlx-calc-poc	Expand objdump DLX ...	2 days ago
openvpn-connect-ec...	Add Firefox Smart Win...	3 days ago
php857-streambuck...	Add PHP 8.5.7 Stream...	yesterday
rustdesk-session-per...	Add RustDesk session ...	2 days ago
systeminformer-phs...	Add System Informer ...	3 days ago
vlc-vp9-reschange-cr...	Add exploitarium arch...	4 days ago
.gitattributes	Add FFmpeg RASC DL...	14 hours ago
.gitignore	Use source-only libssh...	yesterday
README.md	Add FFmpeg RASC DL...	14 hours ago

About

A single archive of public exploit PoCs and vulnerability research writeups. At the time I post these, none have been reported. Feel free to report them yourself and take credit for the CVE if handed out lulz

Readme
Activity
315 stars
16 watching
73 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 2

bikini
we-tech-company

Languages

Python 50.0% C 25.6%
Rust 9.5%
JavaScript 7.0%
PHP 3.9% Shell 2.5%
Other 1.5%

README

If you wish to collaborate/discuss with me, contact me on discord @ashdfrkl

Sharing this repo keeps me motivated to continue dropping 0-days for you all.

Open an issue if you have a specific request for software you want me to take a look at.

Exploitarium

A consolidated archive of my public proof-of-concept and vulnerability research writeups.

Most folders contain one of my former standalone PoC repos, preserved with its original README and tracked files. New research entries are added directly here as self-contained folders.

Contents

Folder	Source
`7zip-rar5-motw-chain-poc`	`bd9533f532c1e4ee6af783b9bb49d1133c`
`anydesk-printer-com-impersonation-poc`	`7491303301093b2d40bee9dadf6b38f757`
`c-ares-tcp-uaf-calc-poc`	direct entry, June 24, 2026
`docker-cp-copyout-destination-escape`	`d1367b1381736d7f961ac808ce88d4e24a`
`firefox-smartwindow-private-url-exfil-poc`	direct entry, June 24, 2026
`floci-apigateway-vtl-rce-poc`	direct entry, June 23, 2026
`flowise-mcp-env-case-bypass-poc`	`ed9fab0086674f1b16467990b33bb9299e`
`ffmpeg-rasc-dlta-calc-poc`	direct entry, June 26, 2026
`ghidra-12.1.2-rce-ace-calc-poc`	`52dee6362990c03c0d753d074c85428824`
`gitea-act-runner-container-options-poc`	`f06d78fb111732f3e7737f4c07e77ef94c`
`imagemagick-gs-delegate-hijack-poc`	`8140e8ee0ed78beaf5e8303a795b70b138`
`libssh2-cve-2026-55200-poc`	direct entry, June 23, 2026
`libssh2-publickey-list-calc-poc`	direct entry, June 25, 2026
`lunar-modrinth-chain-poc`	`ffd02120708b6503f11585858ce3724872`
`mybb-limited-acp-to-admin`	`1610e0373943c2f6562a99f917d3a3d1fd`
`nghttp2-nghttpx-upgrade-queue-poison-poc`	direct entry, June 26, 2026
`nmap-ipv6-extlen-wrap-poc`	direct entry, June 23, 2026
`objdump-dlx-calc-poc`	`7df01e4e20c7375a89e8ccf760526c52eb`
`openvpn-connect-echo-script-ace-poc`	`d2f904d9272d4388c9862131d40e32e072`
`php857-streambucket-soap-rce-rpoc`	direct entry, June 26, 2026

`rustdesk-session-permission-pocs`	direct entry, June 25, 2026
`systeminformer-phsvc-trusted-host-lpe-poc`	direct entry, June 24, 2026
`vlc-vp9-reschange-crash-poc`	`fae72b82f24d03cf2fb9cb55fbb2e7774f`

Consolidation Check

This section applies to the former standalone repositories listed above by commit hash.

The consolidation was checked from fresh GitHub clones on June 23, 2026 before the old standalone repos were removed.

The check compared each former standalone repo's `HEAD` tree against the matching folder here using Git tree data rather than a loose filesystem diff. For every tracked entry, the check required:

- the same relative path;
- the same Git object type;
- the same tree mode, including executable bits;
- the same Git blob ID.

Matching Git blob IDs means the tracked file bytes are identical. The check covered 12 repos and 96 tracked entries with zero mismatches.

This repository preserves the contents of those PoCs. Repository-level metadata such as stars, issues, pull requests, releases, and separate Git history remain in the original repository histories.

Direct entries, including `c-ares-tcp-uaf-calc-poc`, `ffmpeg-rasc-dlta-calc-poc`, `firefox-smartwindow-private-url-exfil-poc`, `floci-apigateway-vtl-rce-poc`, `libssh2-cve-2026-55200-poc`, `libssh2-publickey-list-calc-poc`, `nghttp2-nghttpx-upgrade-queue-poison-poc`, `nmap-ipv6-extlen-wrap-poc`, `php857-streambucket-soap-rce-rpoc`, `rustdesk-session-permission-pocs`, and `systeminformer-phsvc-trusted-host-lpe-poc`, are tracked by this repository's commit history.