CENSUS (/)
IT Security Works

POSTED BY: Angelos T. Kalaitzidis (mailto:akalaitzidis@census-labs.com) / 24.05.2022

# Multiple vulnerabilities in radare2

| | |
|---|---|
| CENSUS ID: | CENSUS-2022-0001 |
| CVE IDs: | CVE-2022-0419 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0419), CVE-2021-44974 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44974), CVE-2021-44975 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44975) |
| Affected Products: | radare2 (https://github.com/radareorg/radare2) versions prior to 5.6.0 |
| Class: | NULL pointer dereference (CWE-476 (https://cwe.mitre.org/data/definitions/476.html)), Heap-based buffer overflow (CWE-122 (https://cwe.mitre.org/data/definitions/122.html)) |
| Discovered by: | Angelos T. Kalaitzidis |

CENSUS identified a number of NULL pointer dereference and Heap buffer overflow bugs in the radare2 (https://rada.re/n/) project code. Radare2 is a popular reverse engineering framework. CENSUS has verified that release 5.6.0 (https://github.com/radareorg/radare2/releases/tag/5.6.0) of radare2 carries the appropriate fixes to remediate all of the identified issues.

## CVE-2022-0419 Vulnerability Details

Function `load_buffer` of `radare2/libr/bin/p/bin_xnu_kernelcache.c` uses a pointer (`obj`) which remains initialized to NULL, when a call to function `get_prelink_info_range_from_mach0()` fails (i.e. returns NULL). The code snippet below shows this problematic code path:

```
static bool load_buffer(RBinFile *bf, void **bin_obj, RBuffer *buf, ut64 loadaddr, Sdb *sdb) {
    ...
189 RKernelCacheObj *obj = NULL; // 1

191 RPrelinkRange *prelink_range = get_prelink_info_range_from_mach0 (main_mach0);
192 if (!prelink_range) {
193     goto beach;              // 2
194 }
....
243 beach:
244 r_buf_free (fbuf);
245 obj->cache_buf = NULL;       // 3
244 MACH0_(mach0_free) (main_mach0);
245 return false;
```

When `get_prelink_info_range_from_mach0()` returns NULL, `obj` remains NULL and the code branches to line 243. There an access to the `obj` pointer is made on line 245, resulting to a NULL pointer dereference and a program crash.

The issue has been patched in version 5.6.0 of radare2.

## CVE-2021-44975 Vulnerability Details

The `objc_build_refs` function is responsible for building the references of a mach-o file as its name suggests. The function can be found out at `/radare2/libr/core/anal_objc.c`

```
static bool objc_build_refs(RCoreObjc *objc) {
        ...

        size_t ss_selrefs = objc->_selrefs->vsize;

        size_t maxsize = R_MAX (ss_const, ss_selrefs); // 1
        maxsize = R_MIN (maxsize, objc->file_size);

        ut8 *buf = calloc (1, maxsize);
        if (!buf) {
                return false;
        }

        ...
        if (!r_io_read_at (objc->core->io, va_selrefs, buf, ss_selrefs)) { // 2
                eprintf ("aao: Cannot read the whole selrefs section\n");
                return false;
        }
        ...
        free (buf);
        return true;
}
```

At comment #1 the `maxsize` quantity is calculated based on the largest value between `ss_const` and `ss_selrefs` (see `R_MAX` macro). Lets consider that the largest of the two is `ss_selrefs`. Then `maxsize` is recalculated based on the lowest value (see `R_MIN` macro) between the previously calculated `maxsize` and `objc->file_size`. Therefore, there may be a case where `ss_selrefs` will be greater than `objc->file_size` and in that case `maxsize` will be equal to `objc->file_size`.

In the above case, buffer `buf` is dynamically allocated with `maxsize` (i.e. `objc->file_size`) bytes. However the `r_io_read_at()` operation at comment #2 will copy `ss_selrefs` bytes to the buffer, resulting to a heap buffer overflow as `ss_selrefs` would be greater than `objc->file_size`.

A similar vulnerability also exists in other code of the same function:

```
        size_t ss_const = objc->_const->vsize;
....
        if (!r_io_read_at (objc->core->io, objc->_const->vaddr, buf, ss_const)) {
                eprintf ("aao: Cannot read the whole const section %zu\n", ss_const);
                return false;
        }
```

Again, `ss_const` can be greater than `objc->file_size` resulting to a heap buffer overflow.

Version 5.6.0 of radare2 comes with the appropriate fix for these issues.

## CVE-2021-44974 Vulnerability Details

A NULL pointer dereference vulnerability exists in the `symbols()` function of `/radare2/libr/bin/bin_symbols.c`.

```
static RList *symbols(RBinFile *bf) {
        RCoreSymCacheElement *element = bf->o->bin_obj;
        ...
        // Parse symbols to a hash table
        for (i = 0; i < element->hdr->n_symbols; i++) {
                RCoreSymCacheElementSymbol *sym = &element->symbols[i]; // 1
                ht_uu_find (hash, sym->paddr, &found);
                if (found) {
                        continue;
                }
                RBinSymbol *s = bin_symbol_from_symbol (element, sym);
                if (s) {
                        r_list_append (res, s);
                }
        }
        ht_uu_free (hash);
        return res;
}
```

As illustrated in the code snippet above, the `element` pointer points to adversary-controlled data (as `bf->o->bin_obj` essentially points to data of the binary file). The `element->symbols` array, is an array of symbols for an object of the file that is being loaded for analysis. In the case where the pointer `element->symbols[0]` is NULL (which is possible as we are talking about adversary-controlled data) the `sym` pointer would also be set to NULL (see comment #1). Then in the next line `sym` is accessed through the `sym->paddr` expression and this leads to a NULL pointer dereference and a program crash.

This issue has been patched in version 5.5.4 of radare2.

## Recommendation

CENSUS advises users to use a radare2 version greater or equal to 5.6.0, as this version carries appropriate patches that remediate correctly all of the aforementioned issues.

## Disclosure Timeline

| | |
|---|---|
| Vendor Contact: | December 7, 2021 |
| CVE Allocation: | December 13, 2021 |
| Vendor Fix Released: | February 2, 2022 |
| Public Advisory: | May 24, 2022 |

Tags: advisories (/news/tag/advisories/) , memory corruption (/news/tag/memory-corruption/) , NULL pointer dereference (/news/tag/null-pointer-dereference/) , buffer overflow (/news/tag/buffer-overflow/) , radare2 (/news/tag/radare2/)



### LATEST ADVISORIES

- Multiple vulnerabilities in radare2 (/news/2022/05/24/multiple-vulnerabilities-in-radare2/)
- WhatsApp exposure of TLS 1.2 cryptographic material to third party apps (/news/2021/04/14/whatsapp-exposure-of-cryptographic-material-to-third-party-apps/)
- Canary Mail and MailCore2 library missing certificate validation check on IMAP STARTTLS (/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/)
- Microchip cryptoauthlib atcab_sign_base buffer overflow (/news/2020/10/21/microchip-cryptoauthlib-atcab_sign_base-buffer-overflow/)
- Microchip cryptoauthlib atcab_genkey_base buffer overflow (/news/2020/10/21/microchip-cryptoauthlib-atcab_genkey_base-buffer-overflow/)

### JOB OPENINGS

- Embedded Security Engineer (/openings/#cfese)
- Vulnerability Researcher (/openings/#cfvr)
- Application Security Engineer (/openings/#cfase)
- Junior IT Security Professional Internship (/openings/#cfina)
- Junior Vulnerability Researcher Internship (/openings/#cfinb)

# IN THE NEWS

- New WhatsApp Bugs Could've Let Attackers Hack Your Phone Remotely (The Hacker News (https://thehackernews.com/2021/04/new-whatsapp-bug-couldve-let-attackers.html), Riscure Security Highlights (https://www.riscure.com/blog/security-highlight-how-hackers-obtain-remote-code-execution-in-whatsapp))
- Mayo Clinic lists CENSUS in recommended external assessors list (https://census-labs.com/news/2018/06/05/census-listed-in-mayo-clinics-recommended-external-assessors-list/) (announcement)
- Microsoft Turns Off Wi-Fi Sense After Risk Revealed (http://www.bankinfosecurity.com/blogs/microsoft-flicks-off-wi-fi-sense-after-attack-revealed-p-2462) (BANK INFO SECURITY)
- NBG Business Seeds Partnership with CENSUS (National Bank of Greece (https://www.nbg.gr/greek/the-group/press-office/press-releases/Pages/sinergasia-nbg-seeds-census.aspx), ERT (https://int.ert.gr/nbg-business-seeds-announces-cooperation-with-census/), FORTUNE Greece (http://www.fortunegreece.com/article/ethniki-trapeza-ke-census-enonoun-tis-dinamis-tous-gia-tin-neofii-epichirimatikotita/))
- Security By Design (http://www.netweek.gr/default.asp?pid=9&la=1&cID=5&arId=31837) (NETWEEK, in greek)
- Wifiphisher: Automating Phishing Attacks Against WiFi Networks (http://www.tripwire.com/state-of-security/off-topic/wifiphisher-automating-phishing-attacks-against-wifi-networks/) (Tripwire)
- DEFCON 22: Hacking Airports, Airplanes and Airwaves (https://web.archive.org/web/20150703133728/https://www.tripwire.com/state-of-security/vulnerability-management/defcon-22-hacking-airports-airplanes-and-airwaves/) (Tripwire - Internet Archive)

## Company News

» FEINDEF 2021 (/news/2021/11/04/feindef-2021/)

» International Cyber Expo 2021 (/news/2021/09/22/ICE2021/)

» OffensiveCon 2020 (/news/2020/07/22/offensivecon-2020/)

## Advisories

» Multiple vulnerabilities in radare2 (/news/2022/05/24/multiple-vulnerabilities-in-radare2/)

» WhatsApp exposure of TLS 1.2 cryptographic material to third party apps (/news/2021/04/14/whatsapp-exposure-of-cryptographic-material-to-third-party-apps/)

» Canary Mail and MailCore2 library missing certificate validation check on IMAP STARTTLS (/news/2021/02/17/canary-mail-app-missing-certificate-validation-check-on-imap-starttls/)

## Blog

» Introducing Janus: a hierarchical multi-blockchain access control system for policy based access to shared resources (/news/2022/06/21/janus-hmbac/)

» Securing the building blocks of embedded software (/news/2021/08/31/securing-the-building-blocks-of-embedded-software/)

» Remote exploitation of a man-in-the-disk vulnerability in WhatsApp (CVE-2021-24027) (/news/2021/04/14/whatsapp-mitd-remote-exploitation-CVE-2021-24027/)