

# A year of fixing Coverity issues all over the Linux kernel

Gustavo A. R. Silva  
[gustavo@embeddedor.com](mailto:gustavo@embeddedor.com)  
@embeddedgus

The Linux Foundation's Core Infrastructure Initiative

Kernel Recipes  
September 26, 2018  
Paris, France

# Agenda

- Coverity.
- Bugfixes.
- Workflow.
- Contributions.
- Results.
- Bonus.

# Coverity

- Static code analyzer.
- Performs analysis without running the code.
- Tons of false positives (This applies to all static code analyzers).

# Coverity high impact issues

- Memory – illegal accesses (out-of-bounds access).
- Resource leaks (memory leaks).
- Uninitialized variables.

# Coverity medium impact issues

- NULL pointer dereferences (before/after null check, explicit null dereference).
- Integer handling issues (bad bit shift operation).
- API usage errors (arguments in wrong order).
- Control flow issues.

# Interface

- <https://scan.coverity.com/projects?utf8=%E2%9C%93&search=linux>

The screenshot displays the Coverity interface for a Linux project. At the top, there's a navigation bar with 'Linux' selected, and options for 'Return to Dashboard', 'Guided Tour', 'Help', and a user profile 'garsilva@embeddedor.com'. Below this, a filter bar shows 'Issues: By Snapshot | Outstanding Defects by category' and 'Filters: Status, Issue Kind, Classification'. The main area features a table of issues:

Category	# Items	CID	Type	Impact	Status	First Detected	Owner	Classification
Memory - corruptions	399	1415670	Explicit null dereferenced	Medium	New	07/24/17	Unassigned	Unclassified
Incorrect expression	439	1415666	Dereference null return value	Medium	New	07/24/17	Unassigned	Unclassified
Memory - illegal accesses	626	1415417	Dereference before null check	Medium	New	07/17/17	Unassigned	Unclassified
Error handling issues	630	1415409	Explicit null dereferenced	Medium	New	07/17/17	Unassigned	Unclassified
Control flow issues	636	1415404	Dereference after null check	Medium	New	07/17/17	Unassigned	Unclassified
Null pointer dereferences	656	1415402	Explicit null dereferenced	Medium	New	07/17/17	Unassigned	Unclassified
Integer handling issues	781	1415400	Dereference after null check	Medium	New	07/17/17	Unassigned	Unclassified

Below the table, it indicates '20 items match' and 'Page 1 of 1'. A code snippet from 'core.c' is shown, with a red box highlighting a 'deref\_ptr: Directly dereferencing pointer ns.' warning. Below the code, a detailed message for CID 1415417 (#1 of 1) states: 'Dereference before null check (REVERSE\_NULL) check\_after\_deref: Null-checking ns suggests that it may be null, but it has already been dereferenced on all paths leading to the check.' The code snippet includes a function 'blk\_status\_t nvme\_setup\_rw' with various initialization and conditional logic.

On the right side, a triage panel for issue 1415417 'Dereference before null check' is visible. It contains fields for 'Classification: Unclassified', 'Severity: Unspecified', 'Action: Undecided', 'Ext. Reference: Type attribute text', and 'Owner: Unassigned'. There is a text area for comments and buttons for 'Apply + Next' and 'Apply'. Below the triage panel, there are sections for 'Projects & Streams', 'Detection History', 'Triage History', and 'Occurrences', with '1: Linux' listed under Occurrences.

Bugfixes

# Fix type of variable

- commit fe78627d430435d22316fe39f2012ece31bf23c2

## Diffstat

```
-rw-r--r-- drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c  
index e2994d337044..111c4921987f 100644
```

```
--- a/drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c  
+++ b/drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c
```

```
@@ -143,7 +143,7 @@ static void wait_for_fbc_state_changed(  
    struct dce110_compressor *cp110,  
    bool enabled)
```

```
{  
-    uint8_t counter = 0;  
+    uint16_t counter = 0;  
    uint32_t addr = mmFBC_STATUS;  
    uint32_t value;
```



# Fix type of variable

- commit 2b6199a1d1b70fccd62aed961ba4c2b979ae499c

```
diff --git a/drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c b/drivers/gpu/drm/
index 9150d26..e2994d3 100644
--- a/drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c
+++ b/drivers/gpu/drm/amd/display/dc/dce110/dce110_compressor.c
@@ -121,10 +121,10 @@ static void reset_lb_on_vblank(struct dc_context *ctx)
     frame_count = dm_read_reg(ctx, mmCRTC_STATUS_FRAME_COUNT);

-     for (retry = 100; retry > 0; retry--) {
+     for (retry = 10000; retry > 0; retry--) {
         if (frame_count != dm_read_reg(ctx, mmCRTC_STATUS_FRAME_COUNT))
             break;
-         msleep(1);
+         udelay(10);
     }
     if (!retry)
         dm_error("Frame count did not increase for 100ms.\n");
@@ -147,14 +147,14 @@ static void wait_for_fbc_state_changed(
     uint32_t addr = mmFBC_STATUS;
     uint32_t value;

-     while (counter < 10) {
+     while (counter < 1000) {
         value = dm_read_reg(cp110->base.ctx, addr);
         if (get_reg_field_value(
             value,
             FBC_STATUS,
             FBC_ENABLE_STATUS) == enabled)
             break;
-         msleep(10);
+         udelay(100);
         counter++;
     }
}
```

# Inconsistent IS\_ERR and PTR\_ERR

- commit 2b7db29b79190f7ad5c32f63594ba08b9b9171ea

## Diffstat

```
-rw-r--r-- drivers/staging/media/imx/imx-media-csi.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/staging/media/imx/imx-media-csi.c b/drivers/staging/media/imx/imx-media-csi.c
index 16cab40156ca..aeab05f682d9 100644
```

```
--- a/drivers/staging/media/imx/imx-media-csi.c
```

```
+++ b/drivers/staging/media/imx/imx-media-csi.c
```

```
@@ -1799,7 +1799,7 @@ static int imx_csi_probe(struct platform_device *pdev)
    priv->dev->of_node = pdata->of_node;
    pinctrl = devm_pinctrl_get_select_default(priv->dev);
    if (IS_ERR(pinctrl)) {
-       ret = PTR_ERR(priv->vdev);
+       ret = PTR_ERR(pinctrl);
        dev_dbg(priv->dev,
                "devm_pinctrl_get_select_default() failed: %d\n", ret);
        if (ret != -ENODEV)
```

# Inconsistent IS\_ERR and PTR\_ERR

- commit 52e17089d1850774d2ef583cdef2b060b84fca8c

```
@@ -1797,6 +1796,10 @@ static int imx_csi_probe(struct platform_device *pdev)
    */
    priv->dev->of_node = pdata->of_node;
    pinctrl = devm_pinctrl_get_select_default(priv->dev);
+   if (IS_ERR(pinctrl)) {
+       ret = PTR_ERR(priv->vdev);
+       goto free;
+   }

    ret = v4l2_async_register_subdev(&priv->sd);
    if (ret)
```

# Logically and structurally dead code

- commit 3f1109d1324405eaeb6c4a586084bd1d933d8b19

## Diffstat

```
-rw-r--r-- drivers/mmc/host/sdhci-cadence.c 4
```

1 files changed, 2 insertions, 2 deletions

```
diff --git a/drivers/mmc/host/sdhci-cadence.c b/drivers/mmc/host/sdhci-cadence.c
index bc30d1637246..7a343b87b5e5 100644
--- a/drivers/mmc/host/sdhci-cadence.c
+++ b/drivers/mmc/host/sdhci-cadence.c
@@ -274,8 +274,8 @@ static int sdhci_cdns_set_tune_val(struct sdhci_host *host, u
         ret = readl_poll_timeout(reg, tmp,
                                 !(tmp & SDHCI_CDNS_HRS06_TUNE_UP),
                                 0, 1);
-
-         return ret;
+         if (ret)
+             return ret;
     }

    return 0;
```

# Logically and structurally dead code

- commit ef6b75671b5f6bfeb5e59e2829643483a3af8c39

```
+      /*  
+      * Workaround for IP errata:  
+      * The IP6116 SD/eMMC PHY design has a timing issue on receive data  
+      * path. Send tune request twice.  
+      */  
+      for (i = 0; i < 2; i++) {  
+          tmp |= SDHCI_CDNS_HRS06_TUNE_UP;  
+          writel(tmp, reg);  
+  
+          ret = readl_poll_timeout(reg, tmp,  
+                                  !(tmp & SDHCI_CDNS_HRS06_TUNE_UP),  
+                                  0, 1);  
+  
+          return ret;  
+      }  
+      return 0;  
+  }
```

# Infinite loop and out-of-bounds access

- commit ad109ba1378679f922f7286e7a9e50e2be778d87

## Diffstat

```
-rw-r--r-- drivers/staging/wilc1000/wilc_wfi_cfgoperations.c 2
```

1 files changed, 1 insertions, 1 deletions

```
diff --git a/drivers/staging/wilc1000/wilc_wfi_cfgoperations.c
index 92322d6f061d..d6401a04fe3f 100644
--- a/drivers/staging/wilc1000/wilc_wfi_cfgoperations.c
+++ b/drivers/staging/wilc1000/wilc_wfi_cfgoperations.c
@@ -608,7 +608,7 @@ wilc_wfi_cfg_alloc_fill_ssid(struct cfg80211
```

out\_free:

```
-     for (i = 0; i < slot_id ; i--)
+     for (i = 0; i < slot_id; i++)
+         kfree(ntwk->net_info[i].ssid);

kfree(ntwk->net_info);
```

# Multiple potential integer overflows

- commit 6f3472a993e7cb63cde5d818dcabc8e42fc03744

## Diffstat

```
-rw-r--r-- drivers/gpu/drm/amd/display/dc/dce/dce_clock_source.c 10
```

1 files changed, 5 insertions, 5 deletions

```
diff --git a/drivers/gpu/drm/amd/display/dc/dce/dce_clock_source.c b/drivers/gpu  
index 88b09dd758ba..ca137757a69e 100644
```

```
--- a/drivers/gpu/drm/amd/display/dc/dce/dce_clock_source.c
```

```
+++ b/drivers/gpu/drm/amd/display/dc/dce/dce_clock_source.c
```

```
@@ -133,7 +133,7 @@ static bool calculate_fb_and_fractional_fb_divider(  
    uint64_t feedback_divider;
```

```
    feedback_divider =
```

```
-        (uint64_t)(target_pix_clk_khz * ref_divider * post_divider);
```

```
+        (uint64_t)target_pix_clk_khz * ref_divider * post_divider;
```

```
    feedback_divider *= 10;
```

```
    /* additional factor, since we divide by 10 afterwards */
```

```
    feedback_divider *= (uint64_t)(calc_pll_cs->fract_fb_divider_factor);
```

```
@@ -203,8 +203,8 @@ static bool calc_fb_divider_checking_tolerance(  
    &fract_feedback_divider);
```

```
    /*Actual calculated value*/
```

```
-    actual_calc_clk_khz = (uint64_t)(feedback_divider *  
-        calc_pll_cs->fract_fb_divider_factor) +
```

```
+    actual_calc_clk_khz = (uint64_t)feedback_divider *  
+        calc_pll_cs->fract_fb_divider_factor +
```

```
        fract_feedback_divider;
```

```
    actual_calc_clk_khz *= calc_pll_cs->ref_freq_khz;
```

```
    actual_calc_clk_khz =
```

# Fix use-after-free

- commit 594619497f3d6d4b8d8440e6d380e8da9dcc9eeb

## Diffstat

```
-rw-r--r-- drivers/net/ethernet/mellanox/mlx5/core/fpga/ipsec.c 3
```

1 files changed, 2 insertions, 1 deletions

```
diff --git a/drivers/net/ethernet/mellanox/mlx5/core/fpga/ipsec.c b/drivers  
index 4f1568528738..0f5da499a223 100644
```

```
--- a/drivers/net/ethernet/mellanox/mlx5/core/fpga/ipsec.c
```

```
+++ b/drivers/net/ethernet/mellanox/mlx5/core/fpga/ipsec.c
```

```
@@ -1061,8 +1061,9 @@ static int fpga_ipsec_fs_create_fte(struct mlx5_core_
```

```
        rule->ctx = mlx5_fpga_ipsec_fs_create_sa_ctx(dev, fte, is_egress);  
        if (IS_ERR(rule->ctx)) {  
+           int err = PTR_ERR(rule->ctx);  
            kfree(rule);  
-           return PTR_ERR(rule->ctx);  
+           return err;  
        }  
  
        rule->fte = fte;
```



# Fix missing return in switch

- commit c5b974bee9d2ceae4c441ae5a01e498c2674e100

## Diffstat

```
-rw-r--r-- drivers/iio/accel/sca3000.c 1 █
```

1 files changed, 1 insertions, 0 deletions

```
diff --git a/drivers/iio/accel/sca3000.c b/drivers/iio/accel/sca3000.c
```

```
index 4dceb75e3586..4964561595f5 100644
```

```
--- a/drivers/iio/accel/sca3000.c
```

```
+++ b/drivers/iio/accel/sca3000.c
```

```
@@ -797,6 +797,7 @@ static int sca3000_write_raw(struct iio_dev *indio_dev,
```

```
        mutex_lock(&st->lock);
```

```
        ret = sca3000_write_3db_freq(st, val);
```

```
        mutex_unlock(&st->lock);
```

```
+        return ret;
```

```
    default:
```

```
        return -EINVAL;
```

```
    }
```

# Workflow

# Workflow

- Review daily Coverity report.

# Workflow

- Review daily Coverity report.
- Build and run Smatch regularly.

# Workflow

- Review daily Coverity report.
- Build and run Smatch regularly.
- Implement and run Coccinelle scripts.

# Workflow

- Review daily Coverity report.
- Build and run Smatch regularly.
- Implement and run Coccinelle scripts.
- Wake up 6AM in the morning.

# Workflow

- Review daily Coverity report.
- Build and run Smatch regularly.
- Implement and run Coccinelle scripts.
- Wake up 6AM in the morning.
- Drink tons of coffee.

# Contributions



# Contributions

200+ patches upstream (KR2017)

# Contributions

200+ patches upstream (KR2017)

750+ patches upstream (KR2018)

# Contributions

- -Wimplicit-fallthrough

# Contributions

- -Wimplicit-fallthrough

```
$ git log --shortstat --author="Gustavo A. R. Silva" | grep fall-through | wc -l
```

274

# Contributions

- -Wimplicit-fallthrough

```
$ git log --shortstat --author="Gustavo A. R.  
Silva" | grep fall-through | wc -l
```

274 (~30%)

# Contributions

- -Wimplicit-fallthrough

```
$ git log --shortstat --author="Gustavo A. R. Silva" | grep fall-through | wc -l
```

274 (~30%)

- Coccinelle (Happy 10<sup>th</sup> anniversary!)

# Contributions

- -Wimplicit-fallthrough

```
$ git log --shortstat --author="Gustavo A. R. Silva" | grep fall-through | wc -l
```

274 (~30%)

- Coccinelle (Happy 10<sup>th</sup> anniversary!)

```
$ git log --shortstat --author="Gustavo A. R. Silva" | grep Coccinelle | wc -l
```

222

# Contributions

- -Wimplicit-fallthrough

```
$ git log --shortstat --author="Gustavo A. R. Silva" | grep fall-through | wc -l
```

274 (~30%)

- Coccinelle (Happy 10<sup>th</sup> anniversary!)

```
$ git log --shortstat --author="Gustavo A. R. Silva" | grep Coccinelle | wc -l
```

222 (~30%)



# Results

# Categories (10+)

- NULL pointer dereferences.
- Spectre vulnerabilities.
- API usage errors.
- Code maintainability issues.
- Constification.
- Control flow issues.
- Uninitialized variables.
- Incorrect expression.
- Integer handling issues.
- Miscellaneous

# Types (38+)

- Variable Length Arrays (VLA)
- Integer overflows
- Bad memory allocation
- Dereference after null check.
- Dereference before null check.
- Dereference null return value.
- Explicit null dereference.
- Missing null check on return value.
- Arguments in wrong order.
- Ignored error return code.
- Unused value.
- Unused code.
- Unnecessary static on local variable.
- Missing return in switch
- Logical vs. bitwise operator
- Wrong operator used
- Spectre V1
- Memory leaks
- 'Constant' variable guards dead code.
- Missing break in switch.
- Uninitialized scalar variable.
- Array compared against 0.
- Identical code for different branches.
- Self assignment.
- Macro compares unsigned to 0.
- Code refactoring.
- Print error message on failure.
- Unnecessary cast on kmalloc.
- Use sizeof(\*var) in kmalloc.
- Double free
- Copy-paste errors
- Read from pointer after free

# Subsystems & Components impacted (38+)

- alsa-devel
- linux-arm-msm
- linux-mediatek
- linux-samsung-soc
- ath10k
- linux-block
- linux-mmc
- linux-scsi
- ceph-devel
- linux-clk
- linux-nfs
- linux-wireless
- linux-media
- cifs-client
- linux-crypto
- linux-omap
- linux-wpan
- dri-devel
- linux-dmaengine
- linux-parisc
- platform-driver-x86
- intel-gfx
- linux-fbdev
- linux-pci
- spi-devel-general
- linux-arm-kernel
- kvm
- linux-fpga
- linux-pm
- target-devel
- linux-acpi
- linux-iio
- linux-rdma
- tpmdd-devel
- linux-rockchip
- linux-input
- linux-renesas-soc
- xen-devel

# Stable trees impacted (14)

- 4.18.y
- 4.17.y
- 4.16.y
- 4.15.y
- 4.14.y \*
- 4.13.y
- 4.12.y
- 4.11.y
- 4.10.y
- 4.9.y
- 4.4.y
- 4.1.y
- 3.18.y
- 3.16.y

**Bonus**

# My experience with CoC

# My experience with CoC

Patchwork Linux Kernel Mailing List Patches Bundles

Show patches with: Submitter = **Gustavo A. R. Silva**  | 1126 patches


- Files changed: 939
- 1126 (interactions in general)



# My experience with CoC

Patchwork Linux Kernel Mailing List

 Patches

 Bundles


Show patches with: Submitter = **Gustavo A. R. Silva**  | 1126 patches

- Files changed: 939
- 1126 (interactions in general)
- 3 stand out

# My experience with CoC

Patchwork Linux Kernel Mailing List

 Patches

 Bundles


Show patches with: Submitter = **Gustavo A. R. Silva**  | 1126 patches

- Files changed: 939
- 1126 (interactions in general)
- 3 stand out
  - “This crap... !!”

# My experience with CoC

Patchwork Linux Kernel Mailing List

 Patches

 Bundles


Show patches with: Submitter = **Gustavo A. R. Silva**  | 1126 patches

- Files changed: 939
- 1126 (interactions in general)
- 3 stand out
  - “This crap... !!”
  - “I hate when... !!”

# My experience with CoC

Patchwork Linux Kernel Mailing List

 Patches


 Bundles


Show patches with: Submitter = **Gustavo A. R. Silva**  | 1126 patches

- Files changed: 939
- 1126 (interactions in general)
- 3 stand out
  - “This crap... !!”
  - “I hate when... !!”
  - Deference

# My experience with CoC

Patchwork Linux Kernel Mailing List

 Patches

 Bundles

Show patches with: Submitter = **Gustavo A. R. Silva**  | 1126 patches

- Files changed: 939
- 1126 (interactions in general)
- 3 stand out
  - “This crap... !!”
  - “I hate when... !!”
  - Deference
- 0.27% (3 out of 1126)

99.73% of a pleasure :P

99.73% of a pleasure :P

Thank you!

[gustavo@embeddedor.com](mailto:gustavo@embeddedor.com)  
@embeddedgus