CVEs are dead, long live the CVE!

Greg Kroah-Hartman

gregkh@linuxfoundation.org
github.com/gregkh/presentation-cve

CVE

Common Vulnerabilities & Exposures

- One identifier for one vulnerability / exposure
- One description for that vulnerability
- Dictionary not a database
- “The way to interoperability and better security coverage”

CVE

Common Vulnerabilities & Exposures

- A string everyone can put in their security builtin

CVE

Better than, “We fixed something described in the second paragraph on the web page over there.”

CVE

Handles the “embedded library in our product has a problem” issue.

CVE

The “cgi plugin remote execution problem.”

CVE

“zlib”

CVE format

CVE-YEAR-NUMBER

CVE-2019-12379

NVD

National Vulnerability Database

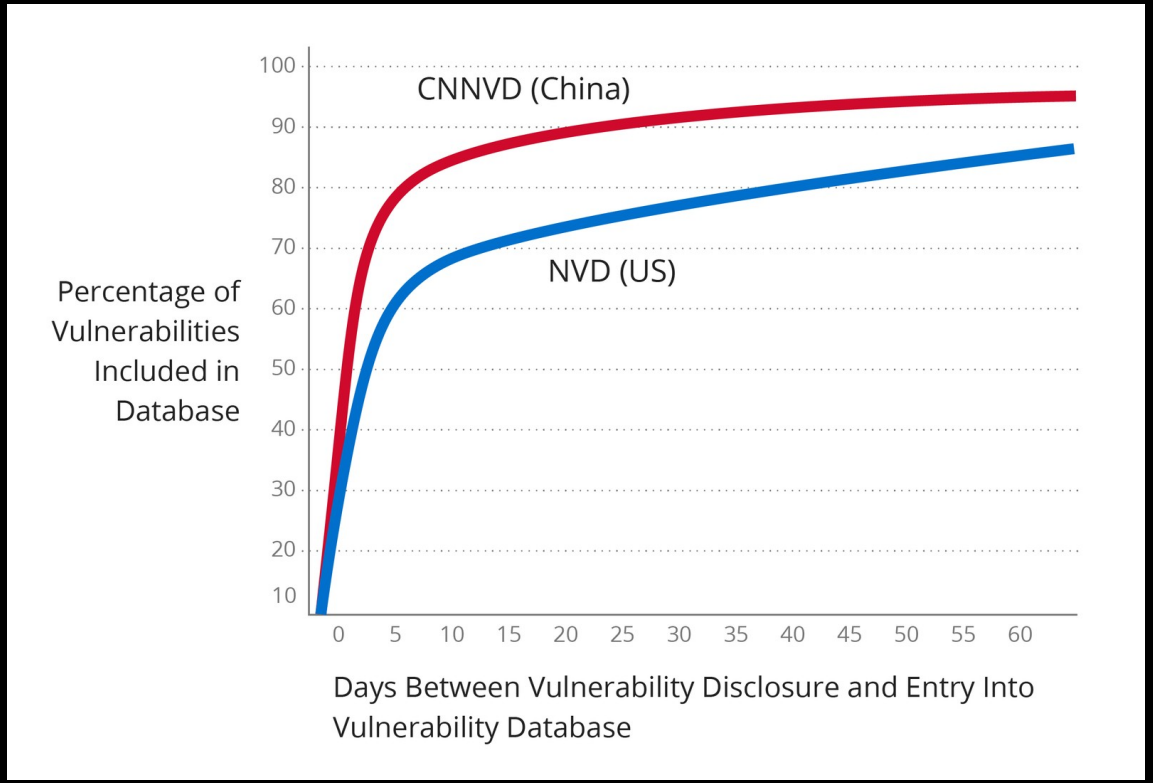
- Superset of CVEs
- Analysis of CVEs
- Gives CVEs a “score”
- Searchable Database
- Slow to update

NVD

"National" Vulnerability Database

CNNVD

China National Vulnerability Database



https://www.recordedfuture.com/chinese-vulnerability-reporting/

CVE/NVD problems

- Missing or rejected vulnerabilities
- Delayed assignment of identifiers
- Poor descriptions of vulnerabilities
- Over/Under-inflated vulnerability scores
- Abuse by engineers to circumvent internal procedures
- Abuse by developers to pad resumes
- Difficulty in revoking invalid identifiers
- Inability to handle ongoing/complex problems requiring multiple fixes over extended periods of time
- Run by USA Government

CVE/NVD problems

- Run by USA Government

CVE/NVD problems

- Inability to handle ongoing/complex problems requiring multiple fixes over extended periods of time
  - Spectre 1 has 1 CVE entry (CVE-2017-5753)
  - Took 10+ original patches
  - 100+ more patches over the past 2 years
  - Still being fixed
  - NVD does NOT point to the fixes needed

CVE/NVD problems

- Abuse by developers to pad resumes
- Difficulty in revoking invalid identifiers

CVE-2019-12379

“An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a memory leak in a certain case of an ENOMEM outcome of kmalloc.”

```
commit 84ecc2f6eb1cb12e6d44818f94fa49b50f06e6ac
Author: Gen Zhang <blackgod016574@gmail.com>
Date:   Thu May 23 08:34:52 2019 +0800

    consolemap: Fix a memory leaking bug in drivers/tty/vt/consolemap.c

    In function con_insert_unipair(), when allocation for p2 and p1[n]
    fails, ENOMEM is returned, but previously allocated p1 is not freed,
    remains as leaking memory. Thus we should free p1 as well when this
    allocation fails.

    Signed-off-by: Gen Zhang <blackgod016574@gmail.com>
    Reviewed-by: Kees Cook <keescook@chromium.org>
    Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

diff --git a/drivers/tty/vt/consolemap.c b/drivers/tty/vt/consolemap.c
index b28aa0d289f8..79fcc96cc7c0 100644
--- a/drivers/tty/vt/consolemap.c
+++ b/drivers/tty/vt/consolemap.c
@@ -489,7 +489,11 @@ con_insert_unipair(struct uni_pagedir *p, u_short unicode, u_short fontpos)
        p2 = p1[n = (unicode >> 6) & 0x1f];
        if (!p2) {
                p2 = p1[n] = kmalloc_array(64, sizeof(u16), GFP_KERNEL);
-               if (!p2) return -ENOMEM;
+               if (!p2) {
+                       kfree(p1);
+                       p->uni_pgdir[n] = NULL;
+                       return -ENOMEM;
+               }
                memset(p2, 0xff, 64*sizeof(u16)); /* No glyphs for the characters (yet) */
        }
```

```
commit 15b3cd8ef46ad1b100e0d3c7e38774f330726820
Author: Ben Hutchings <ben@decadent.org.uk>
Date:   Tue Jun 4 19:00:39 2019 +0100

    Revert "consolemap: Fix a memory leaking bug in drivers/tty/vt/consolemap.c"

    This reverts commit 84ecc2f6eb1cb12e6d44818f94fa49b50f06e6ac.

    con_insert_unipair() is working with a sparse 3-dimensional array:

    - p->uni_pgdir[] is the top layer
    - p1 points to a middle layer
    - p2 points to a bottom layer

    If it needs to allocate a new middle layer, and then fails to allocate
    a new bottom layer, it would previously free only p2, and now it frees
    both p1 and p2.  But since the new middle layer was already registered
    in the top layer, it was not leaked.

    However, if it looks up an *existing* middle layer and then fails to
    allocate a bottom layer, it now frees both p1 and p2 but does *not*
    free any other bottom layers under p1.  So it *introduces* a memory
    leak.

    The error path also cleared the wrong index in p->uni_pgdir[],
    introducing a use-after-free.

    Signed-off-by: Ben Hutchings <ben@decadent.org.uk>
    Fixes: 84ecc2f6eb1c ("consolemap: Fix a memory leaking bug in drivers/tty/vt/consolemap.c")
    Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

diff --git a/drivers/tty/vt/consolemap.c b/drivers/tty/vt/consolemap.c
index 79fcc96cc7c0..b28aa0d289f8 100644
--- a/drivers/tty/vt/consolemap.c
+++ b/drivers/tty/vt/consolemap.c
@@ -489,11 +489,7 @@ con_insert_unipair(struct uni_pagedir *p, u_short unicode, u_short fontpos)
        p2 = p1[n = (unicode >> 6) & 0x1f];
        if (!p2) {
                p2 = p1[n] = kmalloc_array(64, sizeof(u16), GFP_KERNEL);
-               if (!p2) {
-                       kfree(p1);
-                       p->uni_pgdir[n] = NULL;
-                       return -ENOMEM;
-               }
+               if (!p2) return -ENOMEM;
                memset(p2, 0xff, 64*sizeof(u16)); /* No glyphs for the characters (yet) */
        }
```

CVE-2019-12379 timeline

27/05/2019 – CVE published
28/05/2019 – NVD analyzed, score “Medium”
06/06/2019 – Fedora 5.1.6 kernel release
09/06/2019 – Fedora 5.1.7 kernel release
02/07/2019 – *DISPUTED*, link to revert
10/07/2019 – Netapp advisory for 5.1.3 kernel release
(5.1.3 was released 16/05/2019)

CVE-2019-12379 timeline

21/05/2019 – original patch sent to lkml
23/05/2019 – v2 of patch sent based on review
24/05/2019 – v2 of patch sent again (v3???)
24/05/2019 – patch merged to tty-next tree
24/05/2019 – “probably the patch should just be removed…”
27/05/2019 – CVE issued
28/05/2019 – NVD analyzed, score “Medium”
04/06/2019 – Revert patch sent to lkml
04/06/2019 – Revert patch applied to tty-next tree
06/06/2019 – Fedora 5.1.7 kernel release
09/06/2019 – Fedora 5.1.8 kernel release
02/07/2019 – *DISPUTED*, link to revert
10/07/2019 – Netapp advisory for 5.1.3 kernel release
21/07/2019 – 5.3-rc1 is released with patch and revert applied

CVE/NVD problems

- Abuse by engineers to circumvent internal procedures

Linux kernel CVEs

- 2006-2018, 1005 CVEs assigned
  - 41% (414) had a negative “fix date”
  - 12 never fixed
  - Average fix date, -100 days
  - Longest fix dates, -3897 and 2348
  - 88 fixed within 1 week
  - Standard deviation 405 days

Linux bug fixes

- ≈22 a day
- Stable/longterm releases happen 1-2 times a week
- Fully tested as unified release
- Given to you for free!

Linux security fixes

- Happen at least once a week
- Look like any other bugfix
- Many bugs not known to be security “related”
- No differentiation between bug types
  - “bug is a bug is a bug”
- Very few CVEs ever get assigned for kernel issues

Linux security fixes != CVEs

- Small fraction of kernel fixes get CVEs
- If you only cherry-pick CVEs you have an insecure system
- CVEs have follow-on fixes not documented anywhere

If you are not using a supported Linux distribution kernel, or a stable / longterm kernel, you have an insecure system.

If you are not using a ~~supported Linux distribution kernel, or a~~ stable / longterm kernel, you have an insecure system.

“popular phone” - March 2019, 4.14.85

- 8.785 files changed, 3.380.040 lines added, 159.366 lines removed
- Compared to 4.14.108 (May 2019)
  - 1759 patches behind
  - 36 patches taken
    - F2fs, thermal, mm logging cleanups, exynos specific fixes
  - Missed:
    - 12 documented CVEs!
      - HID and networking
    - Bugfixes for mm core, networking vulnerabilities, wireless fixes, HID, f2fs ext4, ARM core, sound, input, USB, spinlock fixes!!!, netfilter, crypto, UFS, video

LTS kernels fix problems

- Bugs are fixed before you realize it
- Google security team requests for Pixel phones in 2018:
  - 92% (201/218) problems were already fixed in an LTS kernel
  - No need for cherry-picking at all
  - Remaining issues were due to out-of-tree code

How to “fix” CVEs

- Ignore them!

How to “fix” CVEs

- Ignore them!
- Burn them down!

How to “fix” CVEs

- Ignore them!
- Burn them down!
- Create something new

Something “new” requirements

- Unique identifier
- Distributed
- Able to be ‘revised’ over time
- Searchable
- Public

```
commit 15b3cd8ef46ad1b100e0d3c7e38774f330726820
Author: Ben Hutchings <ben@decadent.org.uk>
Date:   Tue Jun 4 19:00:39 2019 +0100

    Revert "consolemap: Fix a memory leaking bug in drivers/tty/vt/consolemap.c"

    This reverts commit 84ecc2f6eb1cb12e6d44818f94fa49b50f06e6ac.

    con_insert_unipair() is working with a sparse 3-dimensional array:

    - p->uni_pgdir[] is the top layer
    - p1 points to a middle layer
    - p2 points to a bottom layer

    If it needs to allocate a new middle layer, and then fails to allocate
    a new bottom layer, it would previously free only p2, and now it frees
    both p1 and p2.  But since the new middle layer was already registered
    in the top layer, it was not leaked.

    However, if it looks up an *existing* middle layer and then fails to
    allocate a bottom layer, it now frees both p1 and p2 but does *not*
    free any other bottom layers under p1.  So it *introduces* a memory
    leak.

    The error path also cleared the wrong index in p->uni_pgdir[],
    introducing a use-after-free.

    Signed-off-by: Ben Hutchings <ben@decadent.org.uk>
    Fixes: 84ecc2f6eb1c ("consolemap: Fix a memory leaking bug in drivers/tty/vt/consolemap.c")
    Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>

diff --git a/drivers/tty/vt/consolemap.c b/drivers/tty/vt/consolemap.c
index 79fcc96cc7c0..b28aa0d289f8 100644
--- a/drivers/tty/vt/consolemap.c
+++ b/drivers/tty/vt/consolemap.c
@@ -489,11 +489,7 @@ con_insert_unipair(struct uni_pagedir *p, u_short unicode, u_short fontpos)
```

CVE-ID

CVE-2019-12379 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** DISPUTED ** An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kernel through 5.1.5. There is a memory leak in a certain case of an ENOMEM outcome of kmalloc. NOTE: This id is disputed as not being an issue.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:108478
- URL:http://www.securityfocus.com/bid/108478
- CONFIRM:https://security.netapp.com/advisory/ntap-20190710-0002/
- FEDORA:FEDORA-2019-7ec378191e
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/KLGWJKLMTBBB53D5QLS4HOY2EH246WBE/
- FEDORA:FEDORA-2019-f40bd7826f
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/J36BIJTKEPUOZKJNHQBUZA47RQONUKOI/
- MISC:https://git.kernel.org/pub/scm/linux/kernel/git/gregkh/tty.git/commit/?h=tty-next&id=84ecc2f6eb1cb12e6d44818f94fa49b50f06e6ac
- MISC:https://git.kernel.org/pub/scm/linux/kernel/git/gregkh/tty.git/commit/?h=tty-testing&id=15b3cd8ef46ad1b100e0d3c7e38774f330726820

Assigning CNA

MITRE Corporation

Data Entry Created

```
commit 7caac62ed598a196d6ddf8d9c121e12e082cac3a
Author: Wen Huang <huangwenabc@gmail.com>
Date:   Wed Aug 28 10:07:51 2019 +0800

    mwifiex: Fix three heap overflow at parsing element in cfg80211_ap_settings

    mwifiex_update_vs_ie(),mwifiex_set_uap_rates() and
    mwifiex_set_wmm_params() call memcpy() without checking
    the destination size.Since the source is given from
    user-space, this may trigger a heap buffer overflow.

    Fix them by putting the length check before performing memcpy().

    This fix addresses CVE-2019-14814,CVE-2019-14815,CVE-2019-14816.

    Signed-off-by: Wen Huang <huangwenabc@gmail.com>
    Acked-by: Ganapathi Bhat <gbhat@marvell.comg>
    Signed-off-by: Kalle Valo <kvalo@codeaurora.org>
```

```
commit 941431c491a68e0428bdfb46bbe4cbc52f7bfabb
Author: Wen Huang <huangwenabc@gmail.com>
Date:   Wed Aug 28 10:07:51 2019 +0800

    mwifiex: Fix three heap overflow at parsing element in cfg80211_ap_settings

    commit 7caac62ed598a196d6ddf8d9c121e12e082cac3a upstream.

    mwifiex_update_vs_ie(),mwifiex_set_uap_rates() and
    mwifiex_set_wmm_params() call memcpy() without checking
    the destination size.Since the source is given from
    user-space, this may trigger a heap buffer overflow.

    Fix them by putting the length check before performing memcpy().

    This fix addresses CVE-2019-14814,CVE-2019-14815,CVE-2019-14816.

    Signed-off-by: Wen Huang <huangwenabc@gmail.com>
    Acked-by: Ganapathi Bhat <gbhat@marvell.comg>
    Signed-off-by: Kalle Valo <kvalo@codeaurora.org>
    Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

```
commit 52f6f9d74f31078964ca1574f7bb612da7877ac8
Author: Jann Horn <jannh@google.com>
Date:   Tue Mar 26 23:03:48 2019 +0100

    floppy: fix usercopy direction

    As sparse points out, these two copy_from_user() should actually be
    copy_to_user().

    Fixes: 229b53c9bf4e ("take floppy compat ioctls to sodding floppy.c")
    Cc: stable@vger.kernel.org
    Acked-by: Alexander Popov <alex.popov@linux.com>
    Reviewed-by: Mukesh Ojha <mojha@codeaurora.org>
    Signed-off-by: Jann Horn <jannh@google.com>
    Signed-off-by: Jens Axboe <axboe@kernel.dk>
```

```
commit c3817ffb10369fac0979f0c4367159c412ccc3d8
Author: Jann Horn <jannh@google.com>
Date:   Tue Mar 26 23:03:48 2019 +0100

    floppy: fix usercopy direction

    commit 52f6f9d74f31078964ca1574f7bb612da7877ac8 upstream.

    As sparse points out, these two copy_from_user() should actually be
    copy_to_user().

    Fixes: 229b53c9bf4e ("take floppy compat ioctls to sodding floppy.c")
    Cc: stable@vger.kernel.org
    Acked-by: Alexander Popov <alex.popov@linux.com>
    Reviewed-by: Mukesh Ojha <mojha@codeaurora.org>
    Signed-off-by: Jann Horn <jannh@google.com>
    Signed-off-by: Jens Axboe <axboe@kernel.dk>
    Signed-off-by: Greg Kroah-Hartman <gregkh@linuxfoundation.org>
```

```
$ ~/linux/scripts/fix_in_what_release 7caac62ed598a196d6ddf8d9c121e12e082cac3a
4.4.194 4.9.194 4.14.146 4.19.75 5.2.17 5.3

$ ~/linux/scripts/fix_in_what_release 229b53c9bf4e1132a4aa6feb9632a7a1f1d08c5c
4.4.187 4.9.187 4.13

$ ~/linux/scripts/fix_in_what_release d3252ace0bc6
4.17.19 4.18.5 4.19
```

Something “new” requirements

- Unique identifier
- Distributed
- Able to be ‘revised’ over time
- Searchable
- Public

Git commit id!!!

Marketing to the rescue!

Marketing to the rescue!

- Linux Git Kernel id (LGKI)

Marketing to the rescue!

- Linux Git Kernel id (LGKI)
- Linux Kernel id (LKI)

Marketing to the rescue!

- Linux Git Kernel id (LGKI)
- Linux Kernel id (LKI)
- Kernel Git id (KGI)

Marketing to the rescue!

- Linux Git Kernel id (LGKI)
- Linux Kernel id (LKI)
- Kernel Git id (KGI)
- Git Kernel id (GKI)

Marketing to the rescue!

- Linux Git Kernel id (LGKI)
- Linux Kernel id (LKI)
- Kernel Git id (KGI)
- Git Kernel id (GKI)
- Git Kernel Hash (GKH)

Marketing to the rescue!

- Linux Git Kernel id (LGKI)
- Linux Kernel id (LKI)
- Kernel Git id (KGI)
- Git Kernel id (GKI)
- Git Kernel Hash (GKH)
- Git Hash id (GHI)

Marketing to the rescue!

- Linux Git Kernel id (LGKI)
- Linux Kernel id (LKI)
- Kernel Git id (KGI)
- Git Kernel id (GKI)
- Git Kernel Hash (GKH)
- Git Hash id (GHI)
- Change id (CID)

Change ID

- CID-[12 digit Number]
- CID-7caac62ed598

```
~/linux/stable/linux-stable $ ./generate_cid.sh v4.19..v4.19.1^
CID-0fe5119e267f ("net: bridge: remove ipv6 zero address check in mcast queries")
CID-1f2b5b8e2df4 ("sparc64: Wire up compat getpeername and getsockname.")
CID-5b4fc3882a64 ("sparc64: Make corrupted user stacks more debuggable.")
CID-2b4792eaa9f5 ("sparc64: Export __node_distance.")
CID-713358369382 ("sctp: check policy more carefully when getting pr status")
CID-5ef79151c2fb ("Revert "be2net: remove desc field from be_eq_obj"")
CID-649f0837a8cc ("r8169: fix broken Wake-on-LAN from S5 (poweroff)")
CID-ece23711dd95 ("net: Properly unlink GRO packets on overflow.")
CID-7de414a9dd91 ("net: drop skb on failure in ip_check_defrag()")
CID-a22712a96291 ("mlxsw: core: Fix devlink unregister flow")
CID-ad0b9d94182b ("mlxsw: spectrum_switchdev: Don't ignore deletions of learned MACs")
CID-fb692ec4117f ("net/smc: fix smc_buf_unuse to use the lgr pointer")
CID-4ed591c8ab44 ("net/ipv6: Allow onlink routes to have a device mismatch if it is the default route")
CID-46ebe2834ba5 ("openvswitch: Fix push/pop ethernet validation")
CID-414dd6fb9a1a ("bonding: fix length of actor system")
CID-ff002269a4ee ("vhost: Fix Spectre V1 vulnerability")
CID-da71577545a5 ("rtnetlink: Disallow FDB configuration for non-Ethernet device")
CID-89ab066d4229 ("Revert "net: simplify sock_poll_wait"")
CID-db4f1be3ca9b ("net: udp: fix handling of CHECKSUM_COMPLETE packets")
CID-30549aab146c ("net: stmmac: Fix stmmac_mdio_reset() when building stmmac as modules")
CID-38b4f18d5637 ("net: sched: gred: pass the right attribute to gred_change_table_def()")
CID-d48051c5b837 ("net/mlx5e: fix csum adjustments caused by RXFCS")
CID-ee1abcf68935 ("ipv6/ndisc: Preserve IPv6 control buffer if protocol error handlers are called")
CID-5a2de63fd1a5 ("bridge: do not add port to router list when receives query with source 0.0.0.0")
~/linux/stable/linux-stable $
```

How to “fix” CVEs

- Ignore them!
- Burn them down!
- Create something new

How to “fix” CVEs

- Ignore them!
- Burn them down!
- Create something new
- Re-brand what we have been doing for 14 years

How to “fix” CVEs

- Ignore them!
- Burn them down!
- Create something new
- Re-brand what we have been doing for 14 years

Change ID

- CID-[12 digit Number]
- CID-7caac62ed598

Change ID

- CID-[12 digit Number]
- CID-7caac62ed598