

|                 |                       |
|-----------------|-----------------------|
| Product name    | Confidentiality level |
| B311As-853      | CONFIDENTIAL          |
| Product version | Total 10 pages        |
| V1.0            |                       |

# B311As-853 Firmware Release Notes

## V1.0

|             |                 |      |           |
|-------------|-----------------|------|-----------|
| Prepared by | B311As-853 Team | Date | 2020-3-12 |
| Reviewed by | B311As-853 Team | Date | 2020-3-12 |
| Approved by | B311As-853 Team | Date | 2020-3-12 |



Huawei Technologies Co., Ltd.

All rights reserved

## Revision Record

| Date       | Revision version | FW-WebUI/HiLink Version                               | Change Description           | Author          |
|------------|------------------|-------------------------------------------------------|------------------------------|-----------------|
| 2017-12-5  | 1.0              | FW:6.0.1.3(H100SP4C00)<br>WEBUI 6.0.1.5(W2SP1C03)     | The 1 <sup>st</sup> Version  | B311As-853 Team |
| 2018-1-19  | 2.0              | FW:6.0.1.3(H100SP4C00)<br>WEBUI 6.0.1.5(W2SP1C03)     | The 2 <sup>nd</sup> Version  | B311As-853 Team |
| 2018-1-27  | 3.0              | FW:8.0.1.1(H150SP4C00)<br>WEBUI 8.0.1.3(W2SP3C03)     | The 3 <sup>rd</sup> Version  | B311As-853 Team |
| 2018-3-12  | 4.0              | FW:8.0.1.5(H180SP1C00)<br>WEBUI 8.0.1.13(W2SP1C03)    | The 4 <sup>th</sup> Version  | B311As-853 Team |
| 2018-7-20  | 5.0              | FW:8.0.1.1(H182SP1C00)<br>WEBUI 8.0.1.17(W2SP1C03)    | The 5 <sup>th</sup> Version  | B311As-853 Team |
| 2018-8-23  | 6.0              | FW: 8.0.1.7(H182SP1C00)<br>WEBUI 8.0.1.23(W2SP1C03)   | The 6 <sup>th</sup> Version  | B311As-853 Team |
| 2018-12-13 | 7.0              | FW: 8.0.1.9(H183SP1C00)<br>WEBUI 8.0.1.30(W2SP1C03)   | The 7 <sup>th</sup> Version  | B311As-853 Team |
| 2019-1-11  | 8.0              | FW: 8.0.1.9(H183SP3C00)<br>WEBUI 8.0.1.31(W2SP1C03)   | The 8 <sup>th</sup> Version  | B311As-853 Team |
| 2019-3-27  | 9.0              | FW: 8.0.1.1(H186SP5C00)<br>WEBUI 8.0.1.32(W2SP3C03)   | The 9 <sup>th</sup> Version  | B311As-853 Team |
| 2019-6-3   | 10.0             | FW: 10.0.1.1(H187SP11C00)<br>WEBUI 10.0.1.1(W2SP3C03) | The 10 <sup>th</sup> Version | B311As-853 Team |
| 2019-8-1   | 11.0             | FW: 10.0.1.1(H187SP15C00)<br>WEBUI 10.0.1.1(W2SP5C03) | The 11 <sup>st</sup> Version | B311As-853 Team |
| 2019-10-25 | 12.0             | FW: 10.0.2.1(H690SP1C00)<br>WEBUI 10.0.2.1(W2SP1C03)  | The 12 <sup>st</sup> Version | B311As-853 Team |
| 2020-3-12  | 13.0             | FW: 10.0.2.1(H690SP3C00)<br>WEBUI 10.0.2.1(W2SP2C03)  | The 13 <sup>th</sup> Version | B311As-853 Team |

# Table of Contents

|     |                                            |   |
|-----|--------------------------------------------|---|
| 1   | Main Features .....                        | 4 |
| 2   | Hardware .....                             | 4 |
| 2.1 | Version Description .....                  | 4 |
| 2.2 | Hardware Specifications .....              | 5 |
| 2.3 | Improvements in the Previous Version ..... | 5 |
| 2.4 | Known Limitations and Issues .....         | 5 |
| 3   | Firmware .....                             | 6 |
| 3.1 | Version Description .....                  | 6 |
| 3.2 | Firmware Specifications .....              | 6 |
| 3.3 | Improvement in the Previous Version .....  | 7 |
| 3.4 | Known Limitations and Issues .....         | 7 |
| 4   | WebUI/HiLink .....                         | 7 |
| 4.1 | Version Description .....                  | 7 |
| 4.2 | WebUI/HiLink Specifications .....          | 7 |
| 4.3 | Improvement in the Previous Version .....  | 7 |
| 4.4 | Known Limitations and Issues .....         | 8 |
| 5   | Software Vulnerabilities Fixes .....       | 8 |

## 1 Main Features

The B311As-853 supports the following standards:

- LTE FDD: DL 150Mbps, UL 50Mbps
- LTE TDD: DL 110Mbps, UL 11Mbps
- TDS-CDMA:DL 2.8Mbps,UL 2.2Mbps
- DC-HSPA+: DL 42 Mbps, UL 5.76 Mbps
- HSPA+: DL 21 Mbps (64QAM), UL 5.76 Mbps
- HSPA: DL 14.4 Mbps, UL 5.76 Mbps
- WCDMA PS: DL 384 Kbps, UL 384 Kbps
- WIFI 2.4G:802.11b/g/n,2\*2MIMO 300Mbps
- Equalizer and receive diversity

## 2 Hardware

### 2.1 Version Description

|                     |                     |
|---------------------|---------------------|
| Hardware Version:   | WL2B311M Ver.A      |
| Platform & Chipset: | Balong Hi6921 V7R11 |



## 2.2 Hardware Specifications

| Item                | Specifications                                                                                                                                                            |                                                                                                |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Technical Standard  | LTE                                                                                                                                                                       | 3GPP R9                                                                                        |
|                     | WCDMA                                                                                                                                                                     | 3GPP R8                                                                                        |
|                     | TDS-CDMA                                                                                                                                                                  | 3GPP R9                                                                                        |
| Operating Frequency | LTE                                                                                                                                                                       | Band1,Band3,Band5,Band8 ,Band26,Band28,Band34,B and38,Band39,Band40,Ban d41(Band41: 2545~2655) |
|                     | TDS                                                                                                                                                                       | Band34,Band39                                                                                  |
|                     | UMTS                                                                                                                                                                      | Band1,Band5,Band8                                                                              |
| Memory              | Flash 512MB/DDR 256MB                                                                                                                                                     |                                                                                                |
| WLAN Rate           | 802.11b: 1/2/5.5/11 Mbit/s                                                                                                                                                |                                                                                                |
|                     | 802.11g: 6/9/12/18/24/36/48/54 Mbit/s, compatible 802.11b rate                                                                                                            |                                                                                                |
|                     | 8.2.11n:compatible 802.11b rate and 802.11g rate                                                                                                                          |                                                                                                |
|                     | HT20: Support MCS0–MCS7; Up to 65 Mbit/s.<br>Support MCS8–MCS15; Up to 130 Mbit/s.<br>HT40: Support MCS0–MCS7; Up to 135 Mbit/s.<br>Support MCS8–MCS15; Up to 270 Mbit/s. |                                                                                                |
| External Interfaces | LED: Power/MODE/WLAN/LAN/SIGNAL (3bar)                                                                                                                                    |                                                                                                |
|                     | Ethernet port:1 GE                                                                                                                                                        |                                                                                                |
|                     | SIM/USIM card: 1 2FF                                                                                                                                                      |                                                                                                |
|                     | SMA:1                                                                                                                                                                     |                                                                                                |
| Keys                | 1 Power,1 Reset,1 Wps                                                                                                                                                     |                                                                                                |
| Battery             | NA                                                                                                                                                                        |                                                                                                |
| Ambient Temperature | Operating: 0°C to +40°C<br>Storage: -20°C to +70°C                                                                                                                        |                                                                                                |
| Humidity            | 5% to 95% (non-condensing)                                                                                                                                                |                                                                                                |

## 2.3 Improvements in the Previous Version

| Index                     | Case ID                  | Issue Description |
|---------------------------|--------------------------|-------------------|
| Hardware Version          | WL2B311M Ver.A           |                   |
| Previous Hardware Version | Pre-verification Samples |                   |

## 2.4 Known Limitations and Issues

| Index | Case ID | Issue Description |
|-------|---------|-------------------|
| NA    |         |                   |

## 3 Firmware

### 3.1 Version Description

|                      |                      |
|----------------------|----------------------|
| Firmware Version:    | 10.0.2.1(H690SP3C00) |
| Baseline information | Balong Hi6921 V7R11  |
| OS                   | Linux 3.10.100       |

### 3.2 Firmware Specifications

| Item             | Specifications                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SMS              | <ul style="list-style-type: none"><li>• Writing/Sending/Receiving</li><li>• Sending/Receiving extra-long messages</li><li>• Storage: Up to 500 messages can be saved in the internal memory of the B315s-938.</li><li>• New message prompt</li></ul>                                                                                                                                                                                                                                   |
| WLAN setup       | <ul style="list-style-type: none"><li>• SSID broadcasting and hiding</li><li>• Open system and shared key authentication</li><li>• ASCII and HEX keys</li><li>• 64/128-bit WEP encryption</li><li>• 256-bit WPA-PSK and WPA2-PSK encryption</li><li>• AES encryption algorithm</li><li>• TKIP and AES integrated encryption algorithm</li><li>• Automatic adjustment of ratios</li><li>• Display STA status</li><li>• WLAN MAC filter</li><li>• Guest Wi-Fi</li><li>• Hilink</li></ul> |
| Firewall setup   | <ul style="list-style-type: none"><li>• Firewall Switch</li><li>• LAN IP Filter</li><li>• Virtual Server</li><li>• DMZ Service</li></ul>                                                                                                                                                                                                                                                                                                                                               |
| NAT setup        | <ul style="list-style-type: none"><li>• CONE NAT</li><li>• Symmetric NAT</li><li>• ALG</li><li>• VPN</li></ul>                                                                                                                                                                                                                                                                                                                                                                         |
| DHCP setup       | <ul style="list-style-type: none"><li>• DHCP server enabling and disabling</li><li>• Address pool of the DHCP server setup</li><li>• DHCP lease time setup</li></ul>                                                                                                                                                                                                                                                                                                                   |
| IPv4v6 Dou stack | <ul style="list-style-type: none"><li>• DHCPv4v6 server and client</li><li>• DNSv4 v6server and client</li><li>• Display IPv4v6 WAN address</li></ul>                                                                                                                                                                                                                                                                                                                                  |



| Item               | Specifications                                                                                                                                                                                                                                                                                                                        |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System requirement | <ul style="list-style-type: none"><li>Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8 (does not support Windows RT)</li><li>Mac OS X 10.6, 10.7 and 10.8 with latest upgrades</li><li>Your computer's hardware system should meet or exceed the recommended system requirements for the installed version of OS</li></ul> |

### 3.3 Improvement in the Previous Version

| Index | Case ID | Issue Description |
|-------|---------|-------------------|
| 1     |         |                   |
|       |         |                   |

### 3.4 Known Limitations and Issues

| Index | Case ID | Issue Description |
|-------|---------|-------------------|
|       |         |                   |

## 4 WebUI/HiLink

### 4.1 Version Description

WebUI/HiLink Version: WEBUI 10.0.2.1(W2SP2C03)

### 4.2 WebUI/HiLink Specifications

| Item | Specifications |
|------|----------------|
|      |                |
|      |                |
|      |                |

### 4.3 Improvement in the Previous Version

| Index | Case ID | Issue Description |
|-------|---------|-------------------|
|       |         |                   |
|       |         |                   |
|       |         |                   |



## 4.4 Known Limitations and Issues

| Index | Case ID             | Issue Description |
|-------|---------------------|-------------------|
| 1     | Unrealized Features | DBDC is disabled  |
|       |                     |                   |
|       |                     |                   |

## 5 Software Vulnerabilities Fixes

| Software/Module name   | Version               | CVE ID                         | Vulnerability Description                                                                                                                                                                                                                                                                                                                                               | Impact Description                                                                                                                                                                                                                                                                        |
|------------------------|-----------------------|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">expat</a>  | <a href="#">2.2.6</a> | <a href="#">CVE-2018-20843</a> | <a href="#">In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).</a>                                                                                                   | <a href="https://github.com/libexpat/libexpat/pull/262/commits/11f8838bf99ea0a6f0b76f9760c43704d00c4ff6">https://github.com/libexpat/libexpat/pull/262/commits/11f8838bf99ea0a6f0b76f9760c43704d00c4ff6</a>                                                                               |
| <a href="#">Kernel</a> | <a href="#">4.4</a>   | <a href="#">CVE-2019-12456</a> | <a href="#">An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3sas/mpt3sas_ctl.c in the Linux kernel through 5.1.5. It allows local users to cause a denial of service or possibly have unspecified other impact by changing the value of ioc_number between two kernel reads of that value, aka a "double fetch" vulnerability</a> | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/mkp/scsi.git/commit/?h=5.3/scsi-queue&amp;id=86e5aca7fa2927060839f3e3b40c8bd65a7e8d1e">https://git.kernel.org/pub/scm/linux/kernel/git/mkp/scsi.git/commit/?h=5.3/scsi-queue&amp;id=86e5aca7fa2927060839f3e3b40c8bd65a7e8d1e</a> |
| <a href="#">Kernel</a> | <a href="#">4.4</a>   | <a href="#">CVE-2019-11478</a> | <a href="#">Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service.</a>                                                                                 | <a href="https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md">https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md</a>                                                                                   |
| <a href="#">Kernel</a> | <a href="#">4.4</a>   | <a href="#">CVE-2018-9422</a>  | <a href="#">In get_futex_key of futex.c, there is a use-after-free due to improper locking. This could lead to local escalation of privilege with no additional privileges needed. User interaction is not needed for exploitation</a>                                                                                                                                  | <a href="https://source.android.com/security/bulletin/2018-07-01">https://source.android.com/security/bulletin/2018-07-01</a>                                                                                                                                                             |
| <a href="#">Kernel</a> | <a href="#">4.4</a>   | <a href="#">CVE-2019-13272</a> | <a href="#">In the Linux kernel before 5.1.17, ptrace_link in kernel/ptrace.c mishandles the recording of the credentials of a process that wants to create a ptrace relationship, which allows local users to obtain root access</a>                                                                                                                                   | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6994eefb0053799d2e07cd140df6c2ea106c41ee">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6994eefb0053799d2e07cd140df6c2ea106c41ee</a>                               |



|        |     |                |                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                             |
|--------|-----|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |     |                | by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls <code>execve</code> (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic).                      |                                                                                                                                                                                                                                                             |
| Kernel | 4.4 | CVE-2019-15220 | An issue was discovered in the Linux kernel before 5.2.1. There is a use-after-free caused by a malicious USB device in the <code>drivers/net/wireless/intersil/p54/p54usb.c</code> driver.                                                                                                     | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6e41e2257f1094acc37618bf6c856115374c6922">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6e41e2257f1094acc37618bf6c856115374c6922</a> |
| Kernel | 4.4 | CVE-2019-15219 | An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the <code>drivers/usb/misc/sisusbvga/sisusb.c</code> driver.                                                                                                  | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9a5729f68d3a82786aea110b1bfe610be318f80a">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=9a5729f68d3a82786aea110b1bfe610be318f80a</a> |
| Kernel | 4.4 | CVE-2019-15221 | An issue was discovered in the Linux kernel before 5.1.17. There is a NULL pointer dereference caused by a malicious USB device in the <code>sound/usb/line6/pcm.c</code> driver.                                                                                                               | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3450121997ce872eb7f1248417225827ea249710">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3450121997ce872eb7f1248417225827ea249710</a> |
| Kernel | 4.4 | CVE-2019-15217 | An issue was discovered in the Linux kernel before 5.2.3. There is a NULL pointer dereference caused by a malicious USB device in the <code>drivers/media/usb/zr364xx/zr364xx.c</code> driver.                                                                                                  | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5d2e73a5f80a5b5aff3caf1ec6d39b5b3f54b26e">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5d2e73a5f80a5b5aff3caf1ec6d39b5b3f54b26e</a> |
| Kernel | 4.4 | CVE-2019-12819 | An issue was discovered in the Linux kernel before 5.0. The function <code>__mdio_bus_register()</code> in <code>drivers/net/phy/mdio_bus.c</code> calls <code>put_device()</code> , which will trigger a <code>fixed_mdio_bus_init</code> use-after-free. This will cause a denial of service. | <a href="https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6ff7b060535e87c2ae14dd8548512abfdda528fb">https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6ff7b060535e87c2ae14dd8548512abfdda528fb</a>       |
| Kernel | 4.4 | CVE-2019-15214 | An issue was discovered in the Linux kernel before 5.0.10. There is a use-after-free in the sound subsystem because card disconnection causes certain data structures to be deleted too early. This is related to <code>sound/core/init.c</code> and <code>sound/core/info.c</code> .           | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8c2f870890fd28e023b0fcf49dcee333f2c8bad7">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=8c2f870890fd28e023b0fcf49dcee333f2c8bad7</a> |
| Kernel | 4.4 | CVE-2019-15216 | An issue was discovered in the Linux kernel before 5.0.14. There is a NULL pointer dereference caused by a malicious USB device in the <code>drivers/usb/misc/yurex.c</code> driver.                                                                                                            | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ef61eb43ada6c1d6b94668f0f514e4c268093ff3">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=ef61eb43ada6c1d6b94668f0f514e4c268093ff3</a> |
| Kernel | 4.4 | CVE-2019-15666 | An issue was discovered in the Linux kernel before 5.0.19. There is an out-of-bounds array access in <code>__xfrm_policy_unlink</code> , which will cause denial of service, because <code>verify_newpolicy_info</code> in <code>net/xfrm/xfrm_user.c</code> mishandles directory validation.   | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b805d78d300bcf2c83d6df7da0c818b0fee41427">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=b805d78d300bcf2c83d6df7da0c818b0fee41427</a> |
| Kernel | 4.4 | CVE-2019-3846  | A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the <code>mwifiex</code>                                                                                                                                                                        | <a href="https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.o">https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.o</a>                                                                     |



|        |     |                |                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                |
|--------|-----|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |     |                | kernel module while connecting to a malicious wireless network.                                                                                                                                                                                                                                                                                                                    | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3D5QLS4HOY2EH246WBE/FEDORA-FEDORA-2019-7ec378191e">rg/message/KLGWJKLMTBBB53D5QLS4HOY2EH246WBE/FEDORA-FEDORA-2019-7ec378191e</a>                                        |
| Kernel | 4.4 | CVE-2016-0728  | The <code>join_session_keyring</code> function in <code>security/keys/process_keys.c</code> in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted <code>keyctl</code> commands.                                        | <a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=23567fd052a9abb6d67fe8e7a9ccdd9800a540f2">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=23567fd052a9abb6d67fe8e7a9ccdd9800a540f2</a><br>CONFIRM |
| Kernel | 4.4 | CVE-2019-15213 | An issue was discovered in the Linux kernel before 5.2.3. There is a use-after-free caused by a malicious USB device in the <code>drivers/media/usb/dvb-usb/dvb-usb-init.c</code> driver.                                                                                                                                                                                          | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6cf97230cd5f36b7665099083272595c55d72be7">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=6cf97230cd5f36b7665099083272595c55d72be7</a>    |
| Kernel | 4.4 | CVE-2019-15212 | An issue was discovered in the Linux kernel before 5.1.8. There is a double-free caused by a malicious USB device in the <code>drivers/usb/misc/rio500.c</code> driver.                                                                                                                                                                                                            | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3864d33943b4a76c6e64616280e98d2410b1190f">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=3864d33943b4a76c6e64616280e98d2410b1190f</a>    |
| Kernel | 4.4 | CVE-2019-15215 | An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the <code>drivers/media/usb/cpia2/cpia2_usb.c</code> driver.                                                                                                                                                                                               | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=eff73de2b1600ad8230692f00bc0ab49b166512a">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=eff73de2b1600ad8230692f00bc0ab49b166512a</a>    |
| Kernel | 4.4 | CVE-2019-15218 | An issue was discovered in the Linux kernel before 5.1.8. There is a NULL pointer dereference caused by a malicious USB device in the <code>drivers/media/usb/siano/smsusb.c</code> driver.                                                                                                                                                                                        | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=31e0456de5be379b10fea0fa94a681057114a96e">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=31e0456de5be379b10fea0fa94a681057114a96e</a>    |
| Kernel | 4.4 | CVE-2019-10142 | A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an <code>ioctl</code> was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects. | <a href="https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10142">https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10142</a>                                                                                                                            |
| Kernel | 4.4 | CVE-2019-2054  | In the <code>seccomp</code> implementation prior to kernel version 4.8, there is a possible <code>seccomp</code> bypass due to <code>seccomp</code> policies that allow the use of <code>ptrace</code> . This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.                         | <a href="http://packetstormsecurity.com/files/153799/Kernel-Live-Patch-Security-Notice-LSN-0053-1.html">http://packetstormsecurity.com/files/153799/Kernel-Live-Patch-Security-Notice-LSN-0053-1.html</a>                                                      |
| Kernel | 4.4 | CVE-2019-15211 | An issue was discovered in the Linux kernel before 5.2.6. There is a use-after-free caused by a malicious USB device in the <code>drivers/media/v4l2-core/v4l2-dev.c</code> driver because <code>drivers/media/radio/radio-raremono.c</code> does not properly allocate memory.                                                                                                    | <a href="https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c666355e60ddb4748ead3bdd983e3f7f2224aaf0">https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=c666355e60ddb4748ead3bdd983e3f7f2224aaf0</a>    |
|        |     |                |                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                |