Mentor®
A Siemens Business

Mentor® Embedded Linux® Cumulative Patch Release Notes

Patch 12 Builds 121/150/292/380/381/468

Software Version 2017.02

This document is for information and instruction purposes. Siemens reserves the right to make changes in specifications and other information contained in this publication without prior notice, and the reader should, in all cases, consult Siemens to determine whether any changes have been made.

The terms and conditions governing the sale and licensing of Siemens products are set forth in written agreements between Siemens and its customers. **End User License Agreement with Embedded Software Supplement** — You can print a copy of the EULA with Embedded Software Supplement from: mentor.com/embeddedeula.

No representation or other affirmation of fact contained in this publication shall be deemed to be a warranty or give rise to any liability of Siemens whatsoever.

SIEMENS MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY.

SIEMENS SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, LOST DATA OR PROFITS, EVEN IF SUCH DAMAGES WERE FORESEEABLE, ARISING OUT OF OR RELATED TO THIS PUBLICATION OR THE INFORMATION CONTAINED IN IT, EVEN IF SIEMENS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

LICENSE RIGHTS APPLICABLE TO THE U.S. GOVERNMENT: This document explains the capabilities of commercial products that were developed exclusively at private expense. If the products are acquired directly or indirectly for use by the U.S. Government, then the parties agree that the products and this document are considered "Commercial Items" and "Commercial Computer Software" or "Computer Software Documentation," as defined in 48 C.F.R. §2.101 and 48 C.F.R. §252.227-7014(a)(1) and (a)(5), as applicable. Software and this document may only be used under the terms and conditions of the End User License Agreement referenced above as required by 48 C.F.R. §12.212 and 48 C.F.R §227.7202. The U.S. Government will only have the rights set forth in the End User License Agreement, which supersedes any conflicting terms or conditions in any government order document, except for provisions which are contrary to applicable mandatory federal laws.

TRADEMARKS: The trademarks, logos and service marks ("Marks") used herein are the property of Siemens or other parties. No one is permitted to use these Marks without the prior written consent of Siemens or the owner of the Marks, as applicable. The use herein of third party Marks is not an attempt to indicate Siemens as a source of a product, but is intended to indicate a product from, or associated with, a particular third party. A list of Siemens' trademarks may be viewed at: www.plm.automation.siemens.com/global/en/legal/trademarks.html and mentor.com/trademarks.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

Support Center: support.sw.siemens.com
Send Feedback on Documentation: support.sw.siemens.com/doc_feedback_form

Table of Contents

Chapter 1

Chapter 1
Introduction

This is the cumulative patch release for Mentor® Embedded Linux® (MEL) 2017.02 Patch 12 Builds 121/150/292/380/381/468. It includes fixes for Common Vulnerabilities and Exposures (CVE) and other issues.

Patched Releases

This update patches all MEL components that match the host architecture and version of the update installer. It applies to the following MEL 2017.02 builds and board support packages (BSP).

Build Version	BSP
2017.02.121	Mentor Embedded Linux i.MX6UL
2017.02.121	Mentor Embedded Linux i.MX6 Sabre Series
2017.02.121	Mentor Embedded Linux Cyclone V
2017.02.121	Mentor Embedded Linux T4240/T4160 RDB
2017.02.121	Mentor Embedded Linux MinnowBoard MAX
2017.02.150	Mentor Embedded Linux i.MX6 Sabre Series Update 1
2017.02.292	Mentor Embedded Linux i.MX7D
2017.02.292	Mentor Embedded Linux ZC706
2017.02.292	Mentor Embedded Linux i.MX6ULL
2017.02.380	Mentor Embedded Linux BeagleBone Black AM335x
2017.02.381	Mentor Embedded Linux Advantech UNO 2473G

Build Version	BSP
2017.02.468	Mentor Embedded Linux MPSoC ZCU102 Update 1

Release Information

This patch requires dependencies prior to installation. It also provides a test summary of the issues addressed with this release.

- **Dependencies —** A Mentor Embedded Linux[1] installation with a version that matches this update installer's version.
- **Resolution and Test Summary —** Detailed information for each fix can be found within each update layer *README* file in the following directory: *<mel_install_path>/ mel/<version>/update-mel-<patch#>*

  For example: *$HOME/mgc/embedded/mel/2017.02.468/update-mel-12*

Applying the Fix

Use the update installer to apply the fixes. For more information on installation, consult the *Mentor Embedded Linux Installation Instructions* (*mel_install.pdf*), which you can find in your product documentation directory.

Prerequisites

- A licensed version of MEL for your BSP is installed. See "Patched Releases" on page 5 for the list of supported builds and BSPs.

Procedure

1. Download the highest numbered (patch <*N*>) update installer (*.bin*) that matches the host architecture and version number of the installed MEL BSP:

   ```
   mel-<i686|x64>-<version>-update-<N>.bin
   ```

2. Run the update installer using one of the following methods, and then follow the onscreen prompts:

If you want to...	Enter this command:
Run the installer in graphical user interface (GUI) mode.	`./mel-<i686|x64>-<version>-update-<N>.bin`
Run the installer in console mode.	`./mel-<i686|x64>-<version>-update-<N>.bin –console`

[1] Linux® is a registered trademark of Linus Torvalds in the U.S. and other countries.

Results

When you create build configurations after applying the fixes, they should automatically include the update layers. Existing build configurations detect the fixes and require your confirmation to include the update layers.

Known Problems and Workarounds

This is a known problem and workaround for this release.

Source Files Not Visible

- **Description:** While using the ADE to debug a C/C++ project in the IDE, the source files from the application libraries are not visible.
- **Workaround:** After creating a project in the IDE, follow these steps:

    a. Click **Run** > **Debug Configurations** to open the Debug Configurations window.

    b. Select the debug profile that is automatically created under the Codebench C/C++ Application section in the left side panel.

    c. Select the **Source** tab.

    d. Click **Add** to open the Add Source dialog box.

    e. Double-click **File System Directory**.

    f. Type the target sysroot path in the Directory field or click **Browse** to choose a directory to add.

    ```
    <ADE installation path>/.../sysroots/<target-sysroot>
    ```

    g. Click **OK** to close the Add File System Directory dialog box.

    h. Click **Apply** to close the Debug Configurations window.

    i. Start a debug session and try to step into the code.

Non-CVE Fixes

This cumulative patch addresses the following issues.

DR Number	Description	Fixed In
SB-8703	glibc builds successfully from the recipe but the image recipe fails and displays the following message: “glibc-binary-localedata-en-us” is missing.	Patch #2

DR Number	Description	Fixed In
SB-8801	lttng-modules needs backport of “Fix: nmi-safe clock on 32-bit systems”.	Patch #2
SB-9065	bitbake requests Github credentials while building MEL for Nucleus Master MEL Remote Configuration.	Patch #2
SB-9555	Rebuilding glibc causes error: oe_multilib_header: Unable to find header *bits/syscall.h*.	Patch #2
SB-9694	MEL Dogwood Update-2: QEMU not able to launch for zcu102-zynqmp	Patch #2
SB-9718	MEL Dogwood Update-2: Building core-image-sato failed with 32 bit installer for zcu102-zynqmp.	Patch #2
SB-9738	GPLv3 License Issue in glib-2.0 2.48.2	Patch #2

Kernel Update

This cumulative patch includes kernel updates.

Description	Fixed In
beaglebone-mel, zc706-zynq7-mel, and zcu102-zynqmp-mel (update 1) kernel update from 4.9.197 to 4.9.214	Patch #12
beaglebone-mel, zc706-zynq7-mel, and zcu102-zynqmp-mel (update 1) kernel update from 4.9.189 to 4.9.197	Patch #11
beaglebone-mel and zc706-zynq7-mel kernel update from 4.9.176 to 4.9.189	Patch #10
zcu102-zynqmp-mel (update 1) kernel update from 4.9.174 to 4.9.189	Patch #10
zcu102-zynqmp-mel kernel update from 4.9.155 to 4.9.174	Patch #9
beaglebone-mel kernel update from 4.9.159 to 4.9.176	Patch #9
zc706-zynq7-mel kernel update from 4.9.160 to 4.9.176	Patch #9
mx6q, imx6ulevk-mel, mf0200-mel, and mx6q (update 1) kernel update from 4.1.37 to 4.1.52	Patch #8
mx7d kernel update from 4.1.42 to 4.1.52	Patch #8
i.mx6ullevk-mel kernel update from 4.1.42 to 4.1.52	Patch #8
beaglebone-mel kernel update from 4.9.49 to 4.9.159	Patch #8
zcu102-zynqmp-mel (update 1) kernel update 4.9.72 from 4.9.155	Patch #8

Description	Fixed In
zc706-zynq7-mel kernel update from 4.9 to 4.9.160	Patch #8
cyclone5 kernel update from 4.1.22 ltsi to 4.1.52 lts	Patch #8

List of CVEs

This cumulative patch addresses the following CVEs.

CVE	Description	Package	Fixed In
CVE-2017-12865	Stack-based buffer overflow in "dnsproxy.c" in connman 1.34 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted response query string passed to the "name" variable.	connman 1.33	Patch #12
CVE-2019-1547	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	openssl 1.0.2j	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-1551	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e-dev (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u-dev (Affected 1.0.2-1.0.2t).	openssl 1.0.2j	Patch #12
CVE-2019-1563	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).	openssl 1.0.2j	Patch #12
CVE-2017-3144	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.	dhcp 4.3.4	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-5732	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0	dhcp 4.3.4	Patch #12
CVE-2018-5733	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash. Affects ISC DHCP 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0.	dhcp 4.3.4	Patch #12
CVE-2019-19956	xmlParseBalancedChunkMemoryRecover in parser.c in libxml2 before 2.9.10 has a memory leak related to newDoc->oldNs.	libxml2 2.9.4	Patch #12
CVE-2017-12837	Heap-based buffer overflow in the S_regatom function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (out-of-bounds write) via a regular expression with a '\N{}' escape and the case-insensitive modifier.	perl 5.22.1	Patch #12
CVE-2019-16056	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.	python 2.7.12	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-16935	The documentation XML-RPC server in Python through 2.7.16, 3.x through 3.6.9, and 3.7.x through 3.7.4 has XSS via the server_title field. This occurs in Lib / DocXMLRPCServer.py in Python 2.x, and in Lib/xmlrpc/server.py in Python 3.x. If set_server_title is called with untrusted input, arbitrary JavaScript can be delivered to clients that visit the http URL for this server.	python 2.7.12	Patch #12
CVE-2019-9740	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.	python 2.7.12	Patch #12
CVE-2019-9947	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.	python 2.7.12	Patch #12
CVE-2018-14598	An issue was discovered in XListExtensions in ListExt.c in libX11 through 1.6.5. A malicious server can send a reply in which the first string overflows, causing a variable to be set to NULL that will be freed later on, leading to DoS (segmentation fault).	libx11 1.6.3	Patch #12
CVE-2018-14599	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c is vulnerable to an off-by-one error caused by malicious server responses, leading to DoS or possibly unspecified other impact.	libx11 1.6.3	Patch #12
CVE-2018-14600	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c interprets a variable as signed instead of unsigned, resulting in an out-of-bounds write (of up to 128 bytes), leading to DoS or remote code execution.	libx11 1.6.3	Patch #12

CVE	Description	Package	Fixed In
CVE-2015-7515	The aiptek_probe function in drivers/input/tablet/aiptek.c in the Linux kernel before 4.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device that lacks endpoints.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1	Patch #12
CVE-2015-7885	The dgnc_mgmt_ioctl function in drivers/staging/dgnc/dgnc_mgmt.c in the Linux kernel through 4.3.3 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel memory via a crafted application.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2015-8962	Double free vulnerability in the sg_common_write function in drivers/scsi/sg.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (memory corruption and system crash) by detaching a device during an SG_IO ioctl call.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1	Patch #12
CVE-2015-8963	Race condition in kernel/events/core.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect handling of an swevent data structure during a CPU unplug operation.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2015-8964	The tty_set_termios_ldisc function in drivers/tty/tty_ldisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33	Patch #12
CVE-2017-10662	The sanity_check_raw_super function in fs/f2fs/super.c in the Linux kernel before 4.11.1 does not validate the segment count, which allows local users to gain privileges via unspecified vectors.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.4.105-uno-2473g-mel	Patch #12

CVE	Description	Package	Fixed In
CVE-2017-18509	An issue was discovered in net/ipv6/ip6mr.c in the Linux kernel before 4.11. By setting a specific socket option, an attacker can control a pointer in kernel land and cause an inet_csk_listen_stop general protection fault, or potentially execute arbitrary code under certain circumstances. The issue can be triggered as root (e.g., inside a default LXC container or with the CAP_NET_ADMIN capability) or after namespace unsharing. This occurs because sk_type and protocol are not checked in the appropriate part of the ip6_mroute_* functions. NOTE: this affects Linux distributions that use 4.9.x longterm kernels before 4.9.187.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-12233	In the ea_get function in fs/jfs/xattr.c in the Linux kernel through 4.17.1, a memory corruption bug in JFS can be triggered by calling setxattr twice with two different extended attribute names on the same file. This vulnerability can be triggered by an unprivileged user with the ability to create files and execute programs. A kmalloc call is incorrect, leading to slab-out-of-bounds in jfs_xattr.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-13053	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an integer overflow via a large relative timeout because ktime_add_safe is not used.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-13094	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-13405	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-14609	An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in __del_reloc_root() in fs/btrfs/relocation.c when mounting a crafted btrfs image, related to removing reloc rb_trees when reloc control has not been initialized.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-14617	An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference and panic in hfsplus_lookup() in fs/hfsplus/dir.c when opening a file (that is purportedly a hard link) in an hfs+ filesystem that has malformed catalog data, and is mounted read-only without a metadata directory.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-14734	drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free).	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-18710	An issue was discovered in the Linux kernel through 4.19. An information leak in cdrom_ioctl_select_disc in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940 and CVE-2018-16658.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-19985	The function hso_get_config_data in drivers/net/usb/hso.c in the Linux kernel through 4.19.8 reads if_num from the USB device (as a u8) and uses it to index a small array, resulting in an object out-of-bounds (OOB) read that potentially allows arbitrary read in the kernel address space.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-20976	An issue was discovered in fs/xfs/xfs_super.c in the Linux kernel before 4.18. A use after free exists, related to xfs_fs_fill_super failure.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-21008	An issue was discovered in the Linux kernel before 4.16.7. A use-after-free can be caused by the function rsi_mac80211_detach in the file drivers/net/ wireless/rsi/ rsi_91x_mac80211.c.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-6412	In the function sbusfb_ioctl_helper() in drivers/video/fbdev/sbuslib.c in the Linux kernel through 4.15, an integer signedness error allows arbitrary information leakage for the FBIOPUTCMAP_SPARC and FBIOGETCMAP_SPARC commands.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2018-8043	The unimac_mdio_probe function in drivers/net/phy/mdio-bcm-unimac.c in the Linux kernel through 4.15.8 does not validate certain resource availability, which allows local users to cause a denial of service (NULL pointer dereference).	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2018-8087	Memory leak in the hwsim_new_radio_nl function in drivers/net/wireless/mac80211_hwsim.c in the Linux kernel through 4.15.9 allows local users to cause a denial of service (memory consumption) by triggering an out-of-array error case.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-11833	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent tree block, which might allow local users to obtain sensitive information by reading uninitialized data in the filesystem.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-13631	In parse_hid_report_descriptor in drivers/input/tablet/gtco.c in the Linux kernel through 5.2.1, a malicious USB device can send an HID report that triggers an out-of-bounds write during generation of debugging messages.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-14283	In the Linux kernel before 5.2.3, set_geometry in drivers/block/floppy.c does not validate the sect and head fields, as demonstrated by an integer overflow and out-of-bounds read. It can be triggered by an unprivileged local user when a floppy disk has been inserted. NOTE: QEMU creates the floppy device by default.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-15098	drivers/net/wireless/ath/ath6kl/usb.c in the Linux kernel through 5.2.9 has a NULL pointer dereference via an incomplete address in an endpoint descriptor.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
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 drivers/usb/misc/rio500.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
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 drivers/ media/usb/ dvb-usb/dvb-usb-init.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
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 drivers/ media/usb/cpia2 /cpia2_usb.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
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 drivers/usb/misc/ yurex.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
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 drivers/media/usb/ siano/ smsusb.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
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 drivers/usb/misc/ sisusbvga/ sisusb.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-15291	An issue was discovered in the Linux kernel through 5.2.9. There is a NULL pointer dereference caused by a malicious USB device in the flexcop_usb_probe function in the drivers/media/usb/b2c2/flexcop-usb.c driver.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-15292	An issue was discovered in the Linux kernel before 5.0.9. There is a use-after-free in atalk_proc_exit, related to net/appletalk/atalk_proc.c, net/ appletalk/ddp.c, and net/appletalk/sysctl_net_atalk.c.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-15666	An issue was discovered in the Linux kernel before 5.0.19. There is an out-of-bounds array access in __xfrm_policy_unlink, which will cause denial of service, because verify_newpolicy_info in net/xfrm/xfrm_user.c mishandles directory validation.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-15807	In the Linux kernel before 5.1.13, there is a memory leak in drivers/scsi/ libsas/ sas_expander.c when SAS expander discovery fails. This will cause a BUG and denial of service.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-15916	An issue was discovered in the Linux kernel before 5.0.1. There is a memory leak in register_queue_kobjects() in net/core/net-sysfs.c, which will cause denial of service.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-15926	An issue was discovered in the Linux kernel before 5.2.3. Out of bounds access exists in the functions ath6kl_wmi_pstream_timeout_event_rx and ath6kl_wmi_cac_event_rx in the file drivers/ net/wireless/ath/ath6kl/wmi.c.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-15927	An issue was discovered in the Linux kernel before 4.20.2. An out-of-bounds access exists in the function build_audio_procunit in the file sound/usb/ mixer.c.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-16994	In the Linux kernel before 5.0, a memory leak exists in sit_init_net() in net/ ipv6/sit.c when register_netdev() fails to register sitn->fb_tunnel_dev, which may cause denial of service, aka CID-07f12b26e21a.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-16995	In the Linux kernel before 5.0.3, a memory leak exits in hsr_dev_finalize() in net/hsr/ hsr_device.c if hsr_add_port fails to add a port, which may cause denial of service, aka CID-6caabe7f197d.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-17052	ax25_create in net/ax25/af_ax25.c in the AF_AX25 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-0614e2b73768.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-17053	ieee802154_create in net/ieee802154/socket.c in the AF_IEEE802154 network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-e69dbd4619e7.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-17054	atalk_create in net/appletalk/ddp.c in the AF_APPLETALK network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-6cc03e8aa36c.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-17055	base_sock_create in drivers/isdn/mISDN/socket.c in the AF_ISDN network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-b91ee4aa2a21.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-17056	llcp_sock_create in net/nfc/llcp_sock.c in the AF_NFC network module in the Linux kernel through 5.3.2 does not enforce CAP_NET_RAW, which means that unprivileged users can create a raw socket, aka CID-3a359798b176.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-17133	In the Linux kernel through 5.3.2, cfg80211_mgd_wext_giwessid in net/ wireless/ wext-sme.c does not reject a long SSID IE, leading to a Buffer Overflow.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-18683	An issue was discovered in drivers/media/platform/vivid in the Linux kernel through 5.3.8. It is exploitable for privilege escalation on some Linux distributions where local users have /dev/video0 access, but only if the driver happens to be loaded. There are multiple race conditions during streaming stopping in this driver (part of the V4L2 subsystem). These issues are caused by wrong mutex locking in vivid_stop_generating_vid_cap(), vivid_stop_generating_vid_out(), sdr_cap_stop_streaming(), and the corresponding kthreads. At least one of these race conditions leads to a use-after-free.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-18806	A memory leak in the ql_alloc_large_buffers() function in drivers/net/ethernet /qlogic/qla3xxx.c in the Linux kernel before 5.3.5 allows local users to cause a denial of service (memory consumption) by triggering pci_dma_mapping_error() failures, aka CID-1acb8f2a7a9f.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-18808	A memory leak in the ccp_run_sha_cmd() function in drivers/crypto/ccp/ ccp-ops.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-128c66429247.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19052	A memory leak in the gs_can_open() function in drivers/net/can/usb/gs_usb.c in the Linux kernel before 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering usb_submit_urb() failures, aka CID-fb5be6a7b486.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19054	A memory leak in the cx23888_ir_probe() function in drivers/media/pci/cx23885/ cx23888-ir.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering kfifo_alloc() failures, aka CID-a7b2df76b42b.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19066	A memory leak in the bfad_im_get_stats() function in drivers/scsi/bfa/ bfad_attr.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering bfa_port_get_stats() failures, aka CID-0e62395da2bd.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19073	Memory leaks in drivers/net/wireless/ath/ ath9k/htc_hst.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering wait_for_completion_timeout() failures. This affects the htc_config_pipe_credits() function, the htc_setup_complete() function, and the htc_connect_service() function, aka CID-853acf7caf10.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19074	A memory leak in the ath9k_wmi_cmd() function in drivers/net/wireless/ath/ ath9k/ wmi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-728c1e2a05e4.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19227	In the AppleTalk subsystem in the Linux kernel before 5.1, there is a potential NULL pointer dereference because register_snap_client may return NULL. This will lead to denial of service in net/appletalk/ aarp.c and net/ appletalk/ddp.c, as demonstrated by unregister_snap_client, aka CID-9804501fa122.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19332	An out-of-bounds memory write issue was found in the Linux Kernel, version 3.13 through 5.4, in the way the Linux kernel's KVM hypervisor handled the 'KVM_GET_EMULATED_CPUID' ioctl(2) request to get CPUID features emulated by the KVM hypervisor. A user or process able to access the '/dev/kvm' device could use this flaw to crash the system, resulting in a denial of service.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19524	In the Linux kernel before 5.3.12, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/input/ff-memless.c driver, aka CID-fa3a5a1880c9.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19527	In the Linux kernel before 5.2.10, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/hid/usbhid/hiddev.c driver, aka CID-9c09b214f30e.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19528	In the Linux kernel before 5.3.7, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/misc/iowarrior.c driver, aka CID-edc4746f253d.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19531	In the Linux kernel before 5.2.9, there is a use-after-free bug that can be caused by a malicious USB device in the drivers/usb/misc/yurex.c driver, aka CID-fc05481b2fca.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19533	In the Linux kernel before 5.3.4, there is an info-leak bug that can be caused by a malicious USB device in the drivers/media/ usb/ttusb-dec/ttusb_dec.c driver, aka CID-a10feaf8c464.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19534	In the Linux kernel before 5.3.11, there is an info-leak bug that can be caused by a malicious USB device in the drivers/net/can/ usb/peak_usb/ pcan_usb_core.c driver, aka CID-f7a1337f0d29.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19535	In the Linux kernel before 5.2.9, there is an info-leak bug that can be caused by a malicious USB device in the drivers/net/can/usb/peak_usb/pcan_usb_fd.c driver, aka CID-30a8beeb3042.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19536	In the Linux kernel before 5.2.9, there is an info-leak bug that can be caused by a malicious USB device in the drivers/net/can/usb/peak_usb/pcan_usb_pro.c driver, aka CID-ead16e53c2f0.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19537	In the Linux kernel before 5.2.10, there is a race condition bug that can be caused by a malicious USB device in the USB character device driver layer, aka CID-303911cfc5b9. This affects drivers/usb/core/file.c.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-19965	In the Linux kernel through 5.4.6, there is a NULL pointer dereference in drivers/scsi/libsas/sas_discover.c because of mishandling of port disconnection during discovery, related to a PHY down race condition, aka CID-f70267f379b5.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-19966	In the Linux kernel before 5.1.6, there is a use-after-free in cpia2_exit() in drivers/media/usb/cpia2/cpia2_v4l.c that will cause denial of service, aka CID-dea37a972655.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-20054	In the Linux kernel before 5.0.6, there is a NULL pointer dereference in drop_sysctl_table() in fs/proc/proc_sysctl.c, related to put_links, aka CID-23da9588037e.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-20096	In the Linux kernel before 5.1, there is a memory leak in __feat_register_sp() in net/dccp/feat.c, which may cause denial of service, aka CID-1d3ff0950e2b.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-3459	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-3460	A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33	Patch #12
CVE-2019-3701	An issue was discovered in can_can_gw_rcv in net/can/gw.c in the Linux kernel through 4.19.13. The CAN frame modification rules allow bitwise logical operations that can be also applied to the can_dlc field. The privileged user "root" with CAP_NET_ADMIN can create a CAN frame modification rule that makes the data length code a higher value than the available CAN frame data size. In combination with a configured checksum calculation where the result is stored relatively to the end of the data (e.g. cgw_csum_xor_rel) the tail of the skb (e.g. frag_list pointer in skb_shared_info) can be rewritten which finally can cause a system crash. Because of a missing check, the CAN drivers may write arbitrary content beyond the data registers in the CAN controller's I/O memory when processing can-gw manipulated outgoing frames.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2019-7221	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12
CVE-2019-7222	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.	linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #12

CVE	Description	Package	Fixed In
CVE-2017-16544	In the add_match function in libbb/lineedit.c in BusyBox through 1.27.2, the tab autocomplete feature of the shell, used to get a list of filenames in a directory, does not sanitize filenames and results in executing any escape sequence in the terminal. This could potentially result in code execution, arbitrary file writes, or other attacks.	busybox 1.24.1	Patch #11
CVE-2016-10254	The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted ELF file, which triggers a memory allocation failure.	elfutils 0.166	Patch #11
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted (1) sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.	elfutils 0.166	Patch #11
CVE-2018-18310	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutils through v0.174. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by consider_notes.	elfutils 0.166	Patch #11
CVE-2018-18520	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Although eu-size is intended to support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file.	elfutils 0.166	Patch #11
CVE-2017-7507	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.	gnutls 3.5.3	Patch #11

CVE	Description	Package	Fixed In
CVE-2017-7869	GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk_pkt_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.	gnutls 3.5.3	Patch #11
CVE-2019-18408	archive_read_format_rar_read_data in archive_read_support_format_rar.c in libarchive before 3.4.0 has a use-after-free in a certain ARCHIVE_FAILED situation, related to Ppmd7_DecodeSymbol.	libarchive 3.2.1	Patch #11
CVE-2016-10195	The name_parse function in evdns.c in libevent before 2.1.6-beta allows remote attackers to have unspecified impact via vectors involving the label_len variable, which triggers an out-of-bounds stack read.	libevent 2.0.22	Patch #11
CVE-2016-10196	Stack-based buffer overflow in the evutil_parse_sockaddr_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip_as_string argument.	libevent 2.0.22	Patch #11
CVE-2016-10197	The search_make_new function in evdns.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (out-of-bounds read) via an empty hostname.	libevent 2.0.22	Patch #11
CVE-2017-0379	Libgcrypt before 1.8.1 does not properly consider Curve25519 side-channel attacks, which makes it easier for attackers to discover a secret key, related to cipher/ecc.c and mpi/ec.c.	libgcrypt 1.7.3	Patch #11
CVE-2017-9526	In Libgcrypt before 1.7.7, an attacker who learns the EdDSA session key (from side-channel observation during the signing process) can easily recover the long-term secret key. 1.7.7 makes a cipher/ecc-eddsa.c change to store this session key in secure memory, to ensure that constant-time point operations are used in the MPI library.	libgcrypt 1.7.3	Patch #11

CVE	Description	Package	Fixed In
CVE-2018-14404	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.	libxml2 2.9.4	Patch #11
CVE-2018-12015	In Perl through 5.26.2, the Archive::Tar module allows remote attackers to bypass a directory-traversal protection mechanism, and overwrite arbitrary files, via an archive file containing a symlink and a regular file with the same name.	perl 5.22.1	Patch #11
CVE-2017-1000158	CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow (and possible arbitrary code execution)	python 2.7.12	Patch #11

CVE	Description	Package	Fixed In
CVE-2018-1000030	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.	python 2.7.12	Patch #11
CVE-2017-12424	In shadow before 4.5, the newusers tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts.	shadow 4.2.1	Patch #11

CVE	Description	Package	Fixed In
CVE-2018-1000876	binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.	binutils 2.27	Patch #10
CVE-2019-12900	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.	bzip2 1.0.6	Patch #10
CVE-2019-12749	dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~ /.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass.	dbus 1.10.10	Patch #10

CVE	Description	Package	Fixed In
CVE-2016-7055	There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.0 before 1.1.0c that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected.	openssl 1.0.2j	Patch #10
CVE-2018-20852	http.cookiejar.DefaultPolicy.domain_return_ok in Lib/http/cookiejar.py in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., pythonicexample.com to steal cookies for example.com). When a program uses http.cookiejar.DefaultPolicy and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.	python 2.7.12	Patch #10
CVE-2019-9948	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen ('local_file:///etc/passwd') call.	python 2.7.12	Patch #10

CVE	Description	Package	Fixed In
CVE-2018-16866	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.	systemd 230	Patch #10
CVE-2019-12818	An issue was discovered in the Linux kernel before 4.20.15. The nfc_llcp_build_tlv function in net/nfc/llcp_commands.c may return NULL. If the caller does not check for this, it will trigger a NULL pointer dereference. This will cause denial of service. This affects nfc_llcp_build_gb in net/nfc/llcp_core.c.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #10

CVE	Description	Package	Fixed In
CVE-2019-12819	An issue was discovered in the Linux kernel before 5.0. The function __mdiobus_register() in drivers/net/phy/mdio_bus.c calls put_device(), which will trigger a fixed_mdio_bus_init use-after-free. This will cause a denial of service.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #10
CVE-2019-12984	A NULL pointer dereference vulnerability in the function nfc_genl_deactivate_target() in net/nfc/netlink.c in the Linux kernel before 5.1.13 can be triggered by a malicious user-mode program that omits certain NFC attributes, leading to denial of service.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #10

CVE	Description	Package	Fixed In
CVE-2019-13272	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 by leveraging certain scenarios with a parent-child process relationship, where a parent drops privileges and calls execve (potentially allowing control by an attacker). One contributing factor is an object lifetime issue (which can also cause a panic). Another contributing factor is incorrect marking of a ptrace relationship as privileged, which is exploitable through (for example) Polkit's pkexec helper with PTRACE_TRACEME. NOTE: SELinux deny_ptrace might be a usable workaround in some environments.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-15594	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.	linux-altera-ltsi_4.1.52	Patch #10
CVE-2018-18690	In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition during an xfs attribute change, because xfs_attr_shortform_addname in fs/xfs/libxfs/xfs_attr.c mishandles ATTR_REPLACE operations with conversion of an attr from short to long form.	linux-altera-ltsi_4.1.52	Patch #10

CVE	Description	Package	Fixed In
CVE-2019-14284	In the Linux kernel before 5.2.3, drivers/block/floppy.c allows a denial of service by setup_format_params division-by-zero. Two consecutive ioctls can trigger the bug: the first one should set the drive geometry with .sect and .rate values that make F_SECT_PER_TRACK be zero. Next, the floppy format operation should be called. It can be triggered by an unprivileged local user even when a floppy disk has not been inserted. NOTE: QEMU creates the floppy device by default.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #10
CVE-2017-15129	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.11. The function get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a peer network in netns_ids idr, which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local user to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is thought to be unlikely.	linux-mel 4.1.52-imx6ullevk-mel	Patch #10
CVE-2018-10087	The kernel_wait4 function in kernel/exit.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service by triggering an attempted use of the -INT_MIN value.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel	Patch #10

CVE	Description	Package	Fixed In
CVE-2018-10124	The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an INT_MIN argument.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-10881	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-13406	An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/ uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially elevate privileges because kmalloc_array is not used.	linux-mel 4.1.52-imx6ullevk-mel	Patch #10
CVE-2018-7191	In the tun subsystem in the Linux kernel before 4.13.14, dev_get_valid_name is not called before register_netdevice. This allows local users to cause a denial of service (NULL pointer dereference and panic) via an ioctl(TUNSETIFF) call with a dev name containing a / character. This is similar to CVE-2013-4343.	linux-yocto_4.1.33 linux-qoriq_4.1	Patch #10
CVE-2018-7492	A NULL pointer dereference was found in the net/rds/rdma.c __rds_rdma_map() function in the Linux kernel before 4.14.7 allowing local attackers to cause a system panic and a denial-of-service, related to RDS_GET_MR and RDS_GET_MR_FOR_DEST.	linux-yocto_4.1.33 linux-mel_4.4.105-uno-2473g-mel linux-qoriq_4.1	Patch #10
CVE-2015-8956	The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket.	linux-yocto_4.1.33	Patch #10

CVE	Description	Package	Fixed In
CVE-2017-17052	The mm_init function in kernel/fork.c in the Linux kernel before 4.12.10 does not clear the ->exe_file member of a new process's mm_struct, allowing a local attacker to achieve a use-after-free or possibly have unspecified other impact by running a specially crafted program.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2017-17805	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/ salsa20_generic.c) and x86 implementation (arch/x86/crypto/ salsa20_glue.c) of Salsa20 were vulnerable.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2017-17806	The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2017-18204	The ocfs2_setattr function in fs/ocfs2/file.c in the Linux kernel before 4.14.2 allows local users to cause a denial of service (deadlock) via DIO requests.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2017-18255	The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified other impact via a large value, as demonstrated by an incorrect sample-rate calculation.	linux-mel_4.4.105-uno-2473g-mel	Patch #10

CVE	Description	Package	Fixed In
CVE-2017-18257	The __get_data_block function in fs/f2fs/data.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow and loop) via crafted use of the open and fallocate system calls with an FS_IOC_FIEMAP ioctl.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-1068	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-10940	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-1130	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-7480	The blkcg_init_queue function in block/blk-cgroup.c in the Linux kernel before 4.11 allows local users to cause a denial of service (double free) or possibly have unspecified other impact by triggering a creation failure.	linux-mel_4.4.105-uno-2473g-mel	Patch #10
CVE-2018-8781	The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.	linux-mel_4.4.105-uno-2473g-mel	Patch #10

CVE	Description	Package	Fixed In
CVE-2017-1000410	The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of uninitialized stack variables that may be returned to an attacker in their uninitialized state. By manipulating the code flows that precede the handling of these configuration messages, an attacker can also gain some control over which data will be held in the uninitialized stack variables. This can allow him to bypass KASLR, and stack canaries protection - as both pointers and stack canaries may be leaked in this manner. Combining this vulnerability (for example) with the previously disclosed RCE vulnerability in L2CAP configuration parsing (CVE-2017-1000251) may allow an attacker to exploit the RCE against kernels which were built with the above mitigations. These are the specifics of this vulnerability: In the function l2cap_parse_conf_rsp and in the function l2cap_parse_conf_req the following variable is declared without initialization: struct l2cap_conf_efs efs; In addition, when parsing input configuration parameters in both of these functions, the switch case for handling EFS elements may skip the memcpy call that will write to the efs variable: ... case L2CAP_CONF_EFS: if (olen == sizeof(efs)) memcpy(&efs, (void *)val, olen); ... The olen in the above if is attacker controlled, and regardless of that if, in both of these functions the efs variable would eventually be added to the outgoing configuration request that is being built: l2cap_add_conf_opt(&ptr, L2CAP_CONF_EFS, sizeof(efs), (unsigned long) &efs); So by sending a configuration request, or response, that contains an L2CAP_CONF_EFS element, but with an element length that is not sizeof(efs) - the memcpy to the uninitialized efs variable can be avoided, and the uninitialized variable would be returned to the attacker (16 bytes).	linux-qoriq_4.1	Patch #10

CVE	Description	Package	Fixed In
CVE-2018-18311	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	perl 5.22.1	Patch #10
CVE-2018-18312	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.	perl 5.22.1	Patch #10
CVE-2017-6519	avahi-daemon in Avahi through 0.6.32 and 0.7 inadvertently responds to IPv6 unicast queries with source addresses that are not on-link, which allows remote attackers to cause a denial of service (traffic amplification) and may cause information leakage by obtaining potentially sensitive information from the responding device via port-5353 UDP packets. NOTE: this may overlap CVE-2015-2809.	avahi 0.6.32	Patch #9
CVE-2018-1000877	libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-415: Double Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c, parse_codes(), realloc (rar->lzss.window, new_size) with new_size = 0 that can result in Crash/DoS. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.	libarchive 3.2.1	Patch #9
CVE-2018-1000878	libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-416: Use After Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c that can result in Crash/DoS - it is unknown if RCE is possible. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.	libarchive 3.2.1	Patch #9

CVE	Description	Package	Fixed In
CVE-2018-1000880	libarchive version commit 9693801580c0cf7c70e862d305270a16b52826a7 onwards (release v3.2.0 onwards) contains a CWE-20: Improper Input Validation vulnerability in WARC parser - libarchive/archive_read_support_format_warc.c, _warc_read() that can result in DoS - quasi-infinite run time and disk usage from tiny file. This attack appear to be exploitable via the victim must open a specially crafted WARC file.	libarchive 3.2.1	Patch #9
CVE-2019-1000019	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file.	libarchive 3.2.1	Patch #9
CVE-2019-1000020	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack appears to be exploitable via the victim opening a specially crafted ISO9660 file.	libarchive 3.2.1	Patch #9
CVE-2016-4658	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.	libxml2 2.9.4	Patch #9

CVE	Description	Package	Fixed In
CVE-2017-7655	In Eclipse Mosquitto version from 1.0 to 1.4.15, a Null Dereference vulnerability was found in the Mosquitto library which could lead to crashes for those applications using the library.	mosquitto 1.4.8	Patch #9
CVE-2018-12546	In Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) when a client publishes a retained message to a topic, then has its access to that topic revoked, the retained message will still be published to clients that subscribe to that topic in the future. In some applications this may result in clients being able cause effects that would otherwise not be allowed.	mosquitto 1.4.8	Patch #9
CVE-2018-12550	When Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) is configured to use an ACL file, and that ACL file is empty, or contains only comments or blank lines, then Mosquitto will treat this as though no ACL file has been defined and use a default allow policy. The new behaviour is to have an empty ACL file mean that all access is denied, which is not a useful configuration but is not unexpected.	mosquitto 1.4.8	Patch #9
CVE-2018-12551	When Eclipse Mosquitto version 1.0 to 1.5.5 (inclusive) is configured to use a password file for authentication, any malformed data in the password file will be treated as valid. This typically means that the malformed data becomes a username and no password. If this occurs, clients can circumvent authentication and get access to the broker by using the malformed username. In particular, a blank line will be treated as a valid empty username. Other security measures are unaffected. Users who have only used the mosquitto_passwd utility to create and modify their password files are unaffected by this vulnerability.	mosquitto 1.4.8	Patch #9

CVE	Description	Package	Fixed In
CVE-2019-9636	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.	python 2.7.12	Patch #9
CVE-2018-1049	In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.	systemd 230	Patch #9
CVE-2017-18075	crypto/pcrypt.c in the Linux kernel before 4.14.13 mishandles freeing instances, allowing a local user able to access the AF_ALG-based AEAD interface (CONFIG_CRYPTO_USER_API_AEAD) and pcrypt (CONFIG_CRYPTO_PCRYPT) to cause a denial of service (kfree of an incorrect pointer) or possibly have unspecified other impact by executing a crafted sequence of system calls.	linux-mel_4.4.105-uno-2473g-mel	Patch #9

CVE	Description	Package	Fixed In
CVE-2017-18174	In the Linux kernel before 4.7, the amd_gpio_remove function in drivers/ pinctrl/ pinctrl-amd.c calls the pinctrl_unregister function, leading to a double free.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2017-18216	In fs/ocfs2/cluster/nodemanager.c in the Linux kernel before 4.15, local users can cause a denial of service (NULL pointer dereference and BUG) because a required mutex is not used.	linux-mel_4.4.105-uno-2473g-mel	Patch #9
CVE-2017-18222	In the Linux kernel before 4.12, Hisilicon Network Subsystem (HNS) does not consider the ETH_SS_PRIV_FLAGS case when retrieving sset_count data, which allows local users to cause a denial of service (buffer overflow and memory corruption) or possibly have unspecified other impact, as demonstrated by incompatibility between hns_get_sset_count and ethtool_get_strings.	linux-mel_4.4.105-uno-2473g-mel	Patch #9

CVE	Description	Package	Fixed In
CVE-2018-20836	An issue was discovered in the Linux kernel before 4.20. There is a race condition in smp_task_timedout() and smp_task_done() in drivers/scsi/libsas/ sas_expander.c, leading to a use-after-free.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2019-11190	The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exec_creds() is called too late in load_elf_binary() in fs/ binfmt_elf.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9

CVE	Description	Package	Fixed In
CVE-2019-11486	The Siemens R3964 line discipline driver in drivers/tty/n_r3964.c in the Linux kernel before 5.0.8 has multiple race conditions.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2019-11810	An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service, related to a use-after-free.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9

CVE	Description	Package	Fixed In
CVE-2019-11815	An issue was discovered in rds_tcp_kill_sock in net/rds/tcp.c in the Linux kernel before 5.0.8. There is a race condition leading to a use-after-free, related to net namespace cleanup.	linux-mel_4.4.105-uno-2473g-mel	Patch #9
CVE-2019-11884	The do_hidp_sock_ioctl function in net/bluetooth/hidp/sock.c in the Linux kernel before 5.0.15 allows a local user to obtain potentially sensitive information from kernel stack memory via a HIDPCONNADD command, because a name field may not end with a '\0' character.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.4.105-uno-2473g-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2017-15102	The tower_probe function in drivers/usb/misc/legousbtower.c in the Linux kernel before 4.8.1 allows local users (who are physically proximate for inserting a crafted USB device) to gain privileges by leveraging a write-what-where condition that occurs after a race condition and a NULL pointer dereference.	linux-mel 4.1.52-imx6ullevk-mel linux-qoriq_4.1 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9

CVE	Description	Package	Fixed In
CVE-2017-17052	The mm_init function in kernel/fork.c in the Linux kernel before 4.12.10 does not clear the ->exe_file member of a new process's mm_struct, allowing a local attacker to achieve a use-after-free or possibly have unspecified other impact by running a specially crafted program.	linux-mel 4.1.52-imx6ullevk-mel linux-qoriq_4.1 linux-mel_4.1.52-mx7d	Patch #9
CVE-2018-15594	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2018-16276	An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB driver to crash the kernel or potentially escalate privileges.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9

CVE	Description	Package	Fixed In
CVE-2018-16658	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2018-18690	In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition during an xfs attribute change, because xfs_attr_shortform_addname in fs/xfs/libxfs/xfs_attr.c mishandles ATTR_REPLACE operations with conversion of an attr from short to long form.	linux-mel 4.1.52-imx6ullevk-mel linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2018-20511	An issue was discovered in the Linux kernel before 4.18.11. The ipddp_ioctl function in drivers/net/appletalk/ipddp.c allows local users to obtain sensitive kernel address information by leveraging CAP_NET_ADMIN to read the ipddp_route dev and next fields via an SIOCFINDIPDDPRT ioctl call.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9

CVE	Description	Package	Fixed In
CVE-2018-6554	Memory leak in the irda_bind function in net/ irda/af_irda.c and later in drivers/staging/irda/ net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (memory consumption) by repeatedly binding an AF_IRDA socket.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2018-6555	The irda_setsockopt function in net/irda/ af_irda.c and later in drivers/ staging/irda/net/ af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an AF_IRDA socket.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9
CVE-2019-3901	A race condition in perf_event_open() allows local attackers to leak sensitive data from setuid programs. As no relevant locks (in particular the cred_guard_mutex) are held during the ptrace_may_access() call, it is possible for the specified target task to perform an execve() syscall with setuid execution before perf_event_alloc() actually attaches to it, allowing an attacker to bypass the ptrace_may_access() check and the perf_event_exit_task (current) call that is performed in install_exec_creds() during privileged execve() calls. This issue affects kernel versions before 4.8.	linux-mel 4.1.52-imx6ullevk-mel linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-mel_4.1.52-mx6q linux-mel_4.1.52-imx6ulevk-mel linux-mel_4.1.52-mx7d	Patch #9

CVE	Description	Package	Fixed In
CVE-2017-12193	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations.	linux-qoriq_4.1	Patch #9
CVE-2017-15115	The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns is used in a peel-off action, which allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls.	linux-qoriq_4.1	Patch #9
CVE-2017-15129	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.11. The function get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a peer network in netns_ids idr, which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local user to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is thought to be unlikely.	linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1	Patch #9
CVE-2017-16994	The walk_hugetlb_range function in mm/pagewalk.c in the Linux kernel before 4.14.2 mishandles holes in hugetlb ranges, which allows local users to obtain sensitive information from uninitialized kernel memory via crafted use of the mincore() system call.	linux-qoriq_4.1	Patch #9

CVE	Description	Package	Fixed In
CVE-2017-17805	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/ salsa20_generic.c) and x86 implementation (arch/x86/crypto/ salsa20_glue.c) of Salsa20 were vulnerable.	linux-qoriq_4.1	Patch #9
CVE-2017-17806	The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization.	linux-qoriq_4.1	Patch #9
CVE-2017-18079	drivers/input/serio/i8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact because the port->exists value can change after it is validated.	linux-qoriq_4.1	Patch #9
CVE-2017-18203	The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices.	linux-qoriq_4.1	Patch #9
CVE-2017-18204	The ocfs2_setattr function in fs/ocfs2/file.c in the Linux kernel before 4.14.2 allows local users to cause a denial of service (deadlock) via DIO requests.	linux-qoriq_4.1	Patch #9

CVE	Description	Package	Fixed In
CVE-2017-18208	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.	linux-qoriq_4.1	Patch #9
CVE-2017-18221	The __munlock_pagevec function in mm/mlock.c in the Linux kernel before 4.11.4 allows local users to cause a denial of service (NR_MLOCK accounting corruption) via crafted use of mlockall and munlockall system calls.	linux-yocto_4.1.33 linux-qoriq_4.1	Patch #9
CVE-2017-2618	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory.	linux-yocto_4.1.33 linux-qoriq_4.1	Patch #9
CVE-2018-10881	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.	linux-yocto_4.1.33 linux-qoriq_4.1	Patch #9
CVE-2018-20169	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks during the reading of an extra descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.	linux-altera-ltsi_4.1.52 linux-yocto_4.1.33 linux-qoriq_4.1	Patch #9
CVE-2019-9923	pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.	tar 1.29	Patch #9
CVE-2016-7141	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.	curl 7.50.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2016-8615	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.	curl 7.50.1	Patch #8
CVE-2016-8618	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due to an unsafe `size_t` multiplication, on systems using 32 bit `size_t` variables.	curl 7.50.1	Patch #8
CVE-2016-8622	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.	curl 7.50.1	Patch #8
CVE-2016-8624	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them.	curl 7.50.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2017-1000100	When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.	curl 7.50.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2017-1000254	libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and successfully logs in (anonymous or not), it asks the server for the current directory with the `PWD` command. The server then responds with a 257 response containing the path, inside double quotes. The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this directory name, a directory name passed like this but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the name. When libcurl would then later access the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, thinking it was part of the path. A malicious server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is always issued on new FTP connections and the mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this long could suggest that malformed PWD responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in commit [415d2e7cb7](https://github.com/curl/curl/commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also rejects it if not terminated properly with a final double quote.	curl 7.50.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2017-1000257	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.	curl 7.50.1	Patch #8
CVE-2018-1000005	libcurl 7.49.0 to and including 7.57.0 contains an out bounds read in code handling HTTP/2 trailers. It was reported (https://github.com/ curl/curl/pull/ 2231) that reading an HTTP/2 trailer could mess up future trailers since the stored size was one byte less than required. The problem is that the code that creates HTTP/1-like headers from the HTTP/2 trailer data once appended a string like \`:\` to the target buffer, while this was recently changed to \`: \` (a space was added after the colon) but the following math wasn't updated correspondingly. When accessed, the data is read out of bounds and causes either a crash or that the (too large) data gets passed to client write. This could lead to a denial-of-service situation or an information disclosure if someone has a service that echoes back or uses the trailers for something.	curl 7.50.1	Patch #8
CVE-2018-16842	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service.	curl 7.50.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2019-3822	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/ vauth/ ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.	curl 7.50.1	Patch #8
CVE-2018-16062	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.	elfutils 0.166	Patch #8
CVE-2018-14348	libcgroup up to and including 0.41 creates / var/log/cgred with mode 0666 regardless of the configured umask, leading to disclosure of information.	libcgroup 0.41	Patch #8
CVE-2017-2626	It was discovered that libICE before 1.0.9-8 used a weak entropy to generate keys. A local attacker could potentially use this flaw for session hijacking using the information available from the process list.	libice 1.0.9	Patch #8
CVE-2015-9262	_XcursorThemeInherits in library.c in libXcursor before 1.1.15 allows remote attackers to cause denial of service or potentially code execution via a one-byte heap overflow.	libxcursor 1.1.14	Patch #8

CVE	Description	Package	Fixed In
CVE-2018-14621	An infinite loop vulnerability was found in libtirpc before version 1.0.2-rc2. With the port to using poll rather than select, exhaustion of file descriptors would cause the server to enter an infinite loop, consuming a large amount of CPU time and denying service to other clients until restarted.	libtirpc 1.0.1	Patch #8
CVE-2017-15412	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	libxml2 2.9.4	Patch #8
CVE-2018-19052	An issue was discovered in mod_alias_physical_handler in mod_alias.c in lighttpd before 1.4.50. There is potential ../ path traversal of a single directory above an alias target, with a specific mod_alias configuration where the matched alias lacks a trailing '/' character, but the alias target filesystem path does have a trailing '/' character.	lighttpd 1.4.41	Patch #8
CVE-2017-3736	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.	openssl 1.0.2j	Patch #8

CVE	Description	Package	Fixed In
CVE-2018-14647	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.	python 2.7.12	Patch #8
CVE-2018-18384	Info-ZIP UnZip 6.0 has a buffer overflow in list.c, when a ZIP archive has a crafted relationship between the compressed-size value and the uncompressed-size value, because a buffer size is 10 and is supposed to be 12.	unzip 6.0	Patch #8
CVE-2018-15594	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-16276	An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB driver to crash the kernel or potentially escalate privileges.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-16658	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-18386	drivers/tty/n_tty.c in the Linux kernel before 4.14.11 allows local attackers (who are able to access pseudo terminals) to hang/block further usage of any pseudo terminal devices due to an EXTPROC versus ICANON confusion in TIOCINQ.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2018-18690	In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition during an xfs attribute change, because xfs_attr_shortform_addname in fs/xfs/libxfs/xfs_attr.c mishandles ATTR_REPLACE operations with conversion of an attr from short to long form.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-20169	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks during the reading of an extra descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.	linux-mel_4.4.105-uno-2473g-mel	Patch #8
CVE-2018-20511	An issue was discovered in the Linux kernel before 4.18.11. The ipddp_ioctl function in drivers/net/appletalk/ipddp.c allows local users to obtain sensitive kernel address information by leveraging CAP_NET_ADMIN to read the ipddp_route dev and next fields via an SIOCFINDIPDDPRT ioctl call.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-6554	Memory leak in the irda_bind function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (memory consumption) by repeatedly binding an AF_IRDA socket.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-6555	The irda_setsockopt function in net/irda/af_irda.c and later in drivers/ staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an AF_IRDA socket.	linux-mel_4.4.105-uno-2473g-mel linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8

CVE	Description	Package	Fixed In
CVE-2017-1000363	Linux drivers/char/lp.c Out-of-Bounds Write. Due to a missing bounds check, and the fact that parport_ptr integer is static, a 'secure boot' kernel command line adversary (can happen due to bootloader vulns, e.g. Google Nexus 6's CVE-2016-10277, where due to a vulnerability the adversary has partial control over the command line) can overflow the parport_nr array in the following code, by appending many (>LP_NO) 'lp=none' arguments to the command line.	linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2017-18360	In change_port_settings in drivers/usb/serial/io_ti.c in the Linux kernel before 4.11.3, local users could cause a denial of service by division-by-zero in the serial device layer by trying to set very high baud rates.	linux-yocto_4.1.33 linux-qoriq_4.1	Patch #8
CVE-2018-10938	A flaw was found in the Linux kernel present since v4.0-rc1 and through v4.13-rc4. A crafted network packet sent remotely by an attacker may force the kernel to enter an infinite loop in the cipso_v4_optptr() function in net/ipv4 /cipso_ipv4.c leading to a denial-of-service. A certain non-default configuration of LSM (Linux Security Module) and NetLabel should be set up on a system before an attacker could leverage this flaw.	linux-qoriq_4.1	Patch #8
CVE-2017-18269	An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686/multiarch/memcpy-sse2-unaligned.S in the GNU C Library (aka glibc or libc6) 2.21 through 2.27 does not correctly perform the overlapping memory check if the source memory range spans the middle of the address space, resulting in corrupt data being produced by the copy operation. This may disclose information to context-dependent attackers, or result in a denial of service, or, possibly, code execution.	glibc-sourcery	Patch #8

CVE	Description	Package	Fixed In
CVE-2018-11236	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.	glibc-sourcery	Patch #8
CVE-2018-11237	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.	glibc-sourcery	Patch #8
CVE-2009-5064	Backlog_CVEs CVE_links.txt cve.txt CVE.txt des.txt dg_database.sh dg_xcl.py fix.txt NonCVE.txt out_abcd.txt out_abc.txt out_final.txt out_links.txt pack.txt README-mel-cumulative.txt test url.txt DISPUTED Backlog_CVEs CVE_links.txt cve.txt CVE.txt des.txt dg_database.sh dg_xcl.py fix.txt NonCVE.txt out_abcd.txt out_abc.txt out_final.txt out_links.txt pack.txt README-mel-cumulative.txt test url.txt ldd in the GNU C Library (aka glibc or libc6) 2.13 and earlier allows local users to gain privileges via a Trojan horse executable file linked with a modified loader that omits certain LD_TRACE_LOADED_OBJECTS checks. NOTE: the GNU C Library vendor states "This is just nonsense. There are a gazillion other ways to introduce code if people are downloading arbitrary binaries and install them in appropriate directories or set LD_LIBRARY_PATH etc."	glibc-sourcery	Patch #8
CVE-2018-6485	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.	glibc-sourcery	Patch #8

CVE	Description	Package	Fixed In
CVE-2015-8985	The pop_fail_stack function in the GNU C Library (aka glibc or libc6) allows context-dependent attackers to cause a denial of service (assertion failure and application crash) via vectors related to extended regular expression processing.	glibc-sourcery	Patch #8
CVE-2018-0732	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).	openssl 1.0.2j	Patch #7
CVE-2018-1060	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service.	python 2.7.12	Patch #7
CVE-2018-1061	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service.	python 2.7.12	Patch #7
CVE-2018-10811	strongSwan 5.6.0 and older allows Remote Denial of Service because of Missing Initialization of a Variable.	strongswan 5.5.0	Patch #7
CVE-2018-5388	In stroke_socket.c in strongSwan before 5.6.3, a missing packet length check could allow a buffer underflow, which may lead to resource exhaustion and denial of service while reading from the socket.	strongswan 5.5.0	Patch #7

CVE	Description	Package	Fixed In
CVE-2017-2618	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory.	linux-altera-ltsi_4.1.22 linux-ls1_4.1 linux-mel_4.1.37-mx6q linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #7
CVE-2018-10881	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.	linux-altera-ltsi_4.1.22 linux-ls1_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-mel_4.9.50-beaglebone-mel linux-mel_4.9.71-zcu102-zynqmp-mel linux-mel_4.9.72-zcu102-zynqmp-mel linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #7

CVE	Description	Package	Fixed In
CVE-2018-13406	An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/ uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially elevate privileges because kmalloc_array is not used.	linux-altera-ltsi_4.1.22 linux-ls1_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-mel_4.9.50-beaglebone-mel linux-mel_4.4.105-uno-2473g-mel linux-mel_4.9.71-zcu102-zynqmp-mel linux-mel_4.9.72-zcu102-zynqmp-mel linux-qoriq_4.1 linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx linux-yocto_4.1.33	Patch #7
CVE-2016-2053	The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c.	linux-altera-ltsi_4.1.22 linux-ls1_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-qoriq_4.1 linux-yocto_4.1.33	Patch #7

CVE	Description	Package	Fixed In
CVE-2017-7652	In Eclipse Mosquitto 1.4.14, if a Mosquitto instance is set running with a configuration file, then sending a HUP signal to server triggers the configuration to be reloaded from disk. If there are lots of clients connected so that there are no more file descriptors/sockets available (default limit typically 1024 file descriptors on Linux), then opening the configuration file will fail.	mosquitto 1.4.8	Patch #7
CVE-2016-8616	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive comparisons of user name and password with the existing connections. This means that if an unused connection with proper credentials exists for a protocol that has connection-scoped credentials, an attacker can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.	curl 7.50.1	Patch #7
CVE-2016-8617	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit systems if it receives at least 1Gb as input via `CURLOPT_USERNAME`.	curl 7.50.1	Patch #7
CVE-2016-8619	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.	curl 7.50.1	Patch #7
CVE-2016-8620	The 'globbing' feature in curl before version 7.51.0 has a flaw that leads to integer overflow and out-of-bounds read via user controlled input.	curl 7.50.1	Patch #7
CVE-2016-8621	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.	curl 7.50.1	Patch #7
CVE-2016-8623	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.	curl 7.50.1	Patch #7

CVE	Description	Package	Fixed In
CVE-2018-0495	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.	libgcrypt 1.7.3	Patch #7
CVE-2017-12762	In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree.	linux-xlnx_4.9-xilinx	Patch #7
CVE-2017-18202	The __oom_reap_task_mm function in mm/oom_kill.c in the Linux kernel before 4.14.4 mishandles gather operations, which allows attackers to cause a denial of service (TLB entry leak or use-after-free) or possibly have unspecified other impact by triggering a copy_to_user call within a certain time window.	linux-mel_4.9.50-beaglebone-mel linux-xlnx_4.9-xilinx	Patch #7
CVE-2017-7558	A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak happens when these functions fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of the slab data could be leaked to a userspace.	linux-mel_4.9.50-beaglebone-mel linux-xlnx_4.9-xilinx	Patch #7
CVE-2015-8767	net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call.	linux-qoriq_4.1	Patch #7

CVE	Description	Package	Fixed In
CVE-2017-16997	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/ RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.	glibc-sourcery	Patch #6
CVE-2017-15804	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.	glibc-sourcery	Patch #6
CVE-2017-15670	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.	glibc-sourcery	Patch #6
CVE-2017-12133	Use-after-free vulnerability in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) before 2.26 allows remote attackers to have unspecified impact via vectors related to error path.	glibc-sourcery	Patch #6
CVE-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/ TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).	openssl 1.0.2j	Patch #6

CVE	Description	Package	Fixed In
CVE-2017-18258	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.	libxml2 2.9.4	Patch #6
CVE-2018-1000121	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service	curl 7.50.1	Patch #6
CVE-2018-1000122	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage	curl 7.50.1	Patch #6
CVE-2018-1000301	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.	curl 7.50.1	Patch #6
CVE-2017-18255	The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified other impact via a large value, as demonstrated by an incorrect sample-rate calculation.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2018-10087	The kernel_wait4 function in kernel/exit.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service by triggering an attempted use of the -INT_MIN value.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6
CVE-2018-10124	The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an INT_MIN argument.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2018-10675	The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6
CVE-2018-1068	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2018-10940	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6
CVE-2018-1130	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2018-8781	The udl_fb_mmap function in drivers/gpu/ drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-mel_4.1.42-mx7d linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6
CVE-2016-2143	The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted application, related to arch/s390/include/asm/ mmu_context.h and arch/s390/include/asm/pgalloc.h.	linux-xlnx_4.4-xilinx	Patch #6
CVE-2016-2543	The snd_seq_ioctl_remove_events function in sound/core/seq/seq_clientmgr.c in the Linux kernel before 4.4.1 does not verify FIFO assignment before proceeding with FIFO clearing, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted ioctl call.	linux-xlnx_4.4-xilinx	Patch #6
CVE-2016-2544	Race condition in the queue_delete function in sound/core/seq/seq_queue.c in the Linux kernel before 4.4.1 allows local users to cause a denial of service (use-after-free and system crash) by making an ioctl call at a certain time.	linux-xlnx_4.4-xilinx	Patch #6
CVE-2016-2545	The snd_timer_interrupt function in sound/ core/timer.c in the Linux kernel before 4.4.1 does not properly maintain a certain linked list, which allows local users to cause a denial of service (race condition and system crash) via a crafted ioctl call.	linux-xlnx_4.4-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2016-2546	sound/core/timer.c in the Linux kernel before 4.4.1 uses an incorrect type of mutex, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call.	linux-xlnx_4.4-xilinx	Patch #6
CVE-2016-2547	sound/core/timer.c in the Linux kernel before 4.4.1 employs a locking approach that does not consider slave timer instances, which allows local users to cause a denial of service (race condition, use-after-free, and system crash) via a crafted ioctl call.	linux-xlnx_4.4-xilinx	Patch #6
CVE-2016-2549	sound/core/hrtimer.c in the Linux kernel before 4.4.1 does not prevent recursive callback access, which allows local users to cause a denial of service (deadlock) via a crafted ioctl call.	linux-xlnx_4.4-xilinx	Patch #6
CVE-2017-18257	The __get_data_block function in fs/f2fs/data.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow and loop) via crafted use of the open and fallocate system calls with an FS_IOC_FIEMAP ioctl.	linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6
CVE-2018-7480	The blkcg_init_queue function in block/blk-cgroup.c in the Linux kernel before 4.11 allows local users to cause a denial of service (double free) or possibly have unspecified other impact by triggering a creation failure.	linux-xlnx_4.4-xilinx linux-xlnx_4.9-xilinx	Patch #6
CVE-2016-10088	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.	linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2016-10153	The crypto scatterlist API in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging reliance on earlier net/ceph/crypto.c code.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2016-10154	The smbhash function in fs/cifs/smbencrypt.c in the Linux kernel 4.9.x before 4.9.1 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2016-9588	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-18270	In the Linux kernel before 4.13.5, a local user could create keyrings for other users via keyctl commands, setting unwanted defaults or causing a denial of service.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-5546	The freelist-randomization feature in mm/slab.c in the Linux kernel 4.8.x and 4.9.x before 4.9.5 allows local users to cause a denial of service (duplicate freelist entries and system crash) or possibly have unspecified other impact in opportunistic circumstances by leveraging the selection of a large value for a random number.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-5547	drivers/hid/hid-corsair.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2017-5548	drivers/net/ieee802154/atusb.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-8062	drivers/media/usb/dvb-usb/dw2102.c in the Linux kernel 4.9.x and 4.10.x before 4.10.4 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-8063	drivers/media/usb/dvb-usb/cxusb.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-8064	drivers/media/usb/dvb-usb-v2/dvb_usb_core.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-8066	drivers/net/can/usb/gs_usb.c in the Linux kernel 4.9.x and 4.10.x before 4.10.2 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2017-8067	drivers/char/virtio_console.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-8068	drivers/net/usb/pegasus.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2017-8069	drivers/net/usb/rtl8150.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2018-1118	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.	linux-xlnx_4.9-xilinx	Patch #6
CVE-2018-11232	The etm_setup_aux function in drivers/hwtracing/coresight/coresight-etm-perf.c in the Linux kernel before 4.10.2 allows attackers to cause a denial of service (panic) because a parameter is incorrectly used as a local variable.	linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2018-1000026	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..	linux-xlnx_4.9-xilinx	Patch #6

CVE	Description	Package	Fixed In
CVE-2017-1000410	The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of uninitialized stack variables that may be returned to an attacker in their uninitialized state. By manipulating the code flows that precede the handling of these configuration messages, an attacker can also gain some control over which data will be held in the uninitialized stack variables. This can allow him to bypass KASLR, and stack canaries protection - as both pointers and stack canaries may be leaked in this manner. Combining this vulnerability (for example) with the previously disclosed RCE vulnerability in L2CAP configuration parsing (CVE-2017-1000251) may allow an attacker to exploit the RCE against kernels which were built with the above mitigations. These are the specifics of this vulnerability: In the function l2cap_parse_conf_rsp and in the function l2cap_parse_conf_req the following variable is declared without initialization: struct l2cap_conf_efs efs; In addition, when parsing input configuration parameters in both of these functions, the switch case for handling EFS elements may skip the memcpy call that will write to the efs variable: ... case L2CAP_CONF_EFS: if (olen == sizeof(efs)) memcpy(&efs, (void *)val, olen); ... The olen in the above if is attacker controlled, and regardless of that if, in both of these functions the efs variable would eventually be added to the outgoing configuration request that is being built: l2cap_add_conf_opt(&ptr, L2CAP_CONF_EFS, sizeof(efs), (unsigned long) &efs); So by sending a configuration request, or response, that contains an L2CAP_CONF_EFS element, but with an element length that is not sizeof(efs) - the memcpy to the uninitialized efs variable can be avoided, and the uninitialized variable would be returned to the attacker (16 bytes).	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5

CVE	Description	Package	Fixed In
CVE-2017-16914	The "stub_send_ret_submit()" function (drivers/usb/usbip/stub_tx.c) in the Linux Kernel before version 4.14.8, 4.9.71, 4.1.49, and 4.4.107 allows attackers to cause a denial of service (NULL pointer dereference) via a specially crafted USB over IP packet.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-17052	The mm_init function in kernel/fork.c in the Linux kernel before 4.12.10 does not clear the ->exe_file member of a new process's mm_struct, allowing a local attacker to achieve a use-after-free or possibly have unspecified other impact by running a specially crafted program.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-17805	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/ salsa20_generic.c) and x86 implementation (arch/x86/crypto/ salsa20_glue.c) of Salsa20 were vulnerable.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-17806	The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5

CVE	Description	Package	Fixed In
CVE-2017-18079	drivers/input/serio/i8042.c in the Linux kernel before 4.12.4 allows attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact because the port->exists value can change after it is validated.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-18203	The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-18204	The ocfs2_setattr function in fs/ocfs2/file.c in the Linux kernel before 4.14.2 allows local users to cause a denial of service (deadlock) via DIO requests.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-18208	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.	linux-altera-ltsi_4.1.22 linux-mel_4.1.37-mx6q linux-yocto_4.1.33	Patch #5
CVE-2017-18221	The __munlock_pagevec function in mm/mlock.c in the Linux kernel before 4.11.4 allows local users to cause a denial of service (NR_MLOCK accounting corruption) via crafted use of mlockall and munlockall system calls.	linux-mel_4.1.37-mx6q	Patch #5
CVE-2004-2779	id3_utf16_deserialize() in utf16.c in libid3tag through 0.15.1b misparses ID3v2 tags encoded in UTF-16 with an odd number of bytes, triggering an endless loop allocating memory until an OOM condition is reached, leading to denial-of-service (DoS).	libid3tag 0.15.1b	Patch #5
CVE-2017-5130	An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.	libxml2 2.9.4	Patch #5

CVE	Description	Package	Fixed In
CVE-2017-7375	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not request entity substitution, DTD validation, external DTD subset loading, or default DTD attributes). Depending on the context, this may expose a higher-risk attack surface in libxml2 not usually reachable with default parser flags, and expose content from local files, HTTP, or FTP servers (which might be otherwise unreachable).	libxml2 2.9.4	Patch #5
CVE-2017-14632	Xiph.Org libvorbis 1.3.5 allows Remote Code Execution upon freeing uninitialized memory in the function vorbis_analysis_headerout() in info.c when vi->channels<=0, a similar issue to Mozilla bug 550184.	libvorbis 1.3.5	Patch #4
CVE-2016-6301	The recv_and_process_client_pkt function in networking/ntpd.c in busybox allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged NTP packet, which triggers a communication loop.	busybox 1.24.1	Patch #4
CVE-2017-3735	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.	openssl 1.0.2j	Patch #4
CVE-2017-14633	In Xiph.Org libvorbis 1.3.5, an out-of-bounds array read vulnerability exists in the function mapping0_forward() in mapping0.c, which may lead to DoS when operating on a crafted audio file with vorbis_analysis().	libvorbis 1.3.5	Patch #4
CVE-2017-14160	The bark_noise_hybridmp function in psy.c in Xiph.Org libvorbis 1.3.5 allows remote attackers to cause a denial of service (out-of-bounds access and application crash) or possibly have unspecified other impact via a crafted mp4 file.	libvorbis 1.3.5	Patch #4

CVE	Description	Package	Fixed In
CVE-2017-16931	parser.c in libxml2 before 2.9.5 mishandles parameter-entity references because the NEXTL macro calls the xmlParserHandlePEReference function in the case of a '%' character in a DTD name.	libxml2 2.9.4	Patch #4
CVE-2017-1000251	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33	Patch #4
CVE-2017-12193	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33	Patch #4
CVE-2017-15102	The tower_probe function in drivers/usb/misc/legousbtower.c in the Linux kernel before 4.8.1 allows local users (who are physically proximate for inserting a crafted USB device) to gain privileges by leveraging a write-what-where condition that occurs after a race condition and a NULL pointer dereference.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33	Patch #4
CVE-2017-15115	The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns is used in a peel-off action, which allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33	Patch #4
CVE-2017-11550	The id3_ucs4_length function in ucs4.c in libid3tag 0.15.1b allows remote attackers to cause a denial of service (NULL Pointer Dereference and application crash) via a crafted mp3 file.	libid3tag 0.15.1b	Patch #4

CVE	Description	Package	Fixed In
CVE-2017-1000117	A malicious third-party can give a crafted "ssh://..." URL to an unsuspecting victim, and an attempt to visit the URL can result in any program that exists on the victim's machine being executed. Such a URL could be placed in the .gitmodules file of a malicious project, and an unsuspecting victim could be tricked into running "git clone --recurse-submodules" to trigger the vulnerability.	git 2.9.3	Patch #4
CVE-2015-9019	In libxslt 1.1.29 and earlier, the EXSLT math.random function was not initialized with a random seed during startup, which could cause usage of this function to produce predictable outputs.	libxslt 1.1.29	Patch #4
CVE-2017-8779	rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.	libtirpc 1.0.1	Patch #4
CVE-2017-16994	The walk_hugetlb_range function in mm/pagewalk.c in the Linux kernel before 4.14.2 mishandles holes in hugetlb ranges, which allows local users to obtain sensitive information from uninitialized kernel memory via crafted use of the mincore() system call.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33	Patch #4
CVE-2017-8872	The htmlParseTryOrFinish function in HTMLparser.c in libxml2 2.9.4 allows attackers to cause a denial of service (buffer over-read) or information disclosure.	libxml2 2.9.4	Patch #4
CVE-2017-15908	In systemd 223 through 235, a remote DNS server can respond with a custom crafted DNS NSEC resource record to trigger an infinite loop in the dns_packet_read_type_window() function of the 'systemd-resolved' service and cause a DoS of the affected service.	systemd 230	Patch #4

CVE	Description	Package	Fixed In
CVE-2017-16939	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages.	linux-altera-ltsi_4.1.22	Patch #4
CVE-2017-8816	The NTLM authentication feature in curl and libcurl before 7.57.0 on 32-bit platforms allows attackers to cause a denial of service (integer overflow and resultant buffer overflow, and application crash) or possibly have unspecified other impact via vectors involving long user and password fields.	curl 7.50.1	Patch #4
CVE-2017-16612	libXcursor before 1.1.15 has various integer overflows that could lead to heap buffer overflows when processing malicious cursors, e.g., with programs like GIMP. It is also possible that an attack vector exists against the related code in cursor/xcursor.c in Wayland through 1.14.0.	libxcursor 1.1.14	Patch #4

CVE	Description	Package	Fixed In
CVE-2017-3737	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/ encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.	openssl 1.0.2j	Patch #4

CVE	Description	Package	Fixed In
CVE-2017-3738	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.	openssl 1.0.2j	Patch #4
CVE-2017-13077	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.	wpa-supplicant 2.5	Patch #3
CVE-2017-13078	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.	wpa-supplicant 2.5	Patch #3

CVE	Description	Package	Fixed In
CVE-2017-13079	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the four-way handshake, allowing an attacker within radio range to spoof frames from access points to clients.	wpa-supplicant 2.5	Patch #3
CVE-2017-13080	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.	wpa-supplicant 2.5	Patch #3
CVE-2017-13081	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the group key handshake, allowing an attacker within radio range to spoof frames from access points to clients.	wpa-supplicant 2.5	Patch #3
CVE-2017-13082	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.	wpa-supplicant 2.5	Patch #3
CVE-2017-13086	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Tunneled Direct-Link Setup (TDLS) Peer Key (TPK) during the TDLS handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.	wpa-supplicant 2.5	Patch #3
CVE-2017-13087	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.	wpa-supplicant 2.5	Patch #3

CVE	Description	Package	Fixed In
CVE-2017-13088	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.	wpa-supplicant 2.5	Patch #3
CVE-2016-10396	The racoon daemon in IPsec-Tools 0.8.2 contains a remotely exploitable computational-complexity attack when parsing and storing ISAKMP fragments. The implementation permits a remote attacker to exhaust computational resources on the remote endpoint by repeatedly sending ISAKMP fragment packets in a particular order such that the worst-case computational complexity is realized in the algorithm utilized to determine if reassembly of the fragments can take place.	ipsec-tools 0.8.2	Patch #3
CVE-2017-1000381	The c-ares function \`ares_parse_naptr_reply()\`, which is used for parsing NAPTR responses, could be triggered to read memory outside of the given input buffer if the passed in DNS response packet was crafted in a particular way.	c-ares 1.10.0	Patch #3
CVE-2017-7544	libexif through 0.6.21 is vulnerable to out-of-bounds heap read vulnerability in exif_data_save_data_entry function in libexif/exif-data.c caused by improper length computation of the allocated data of an ExifMnote entry which can cause denial-of-service or possibly information disclosure.	libexif 0.6.21	Patch #3
CVE-2017-7650	In Mosquitto before 1.4.12, pattern based ACLs can be bypassed by clients that set their username/client id to '#' or '+'. This allows locally or remotely connected clients to access MQTT topics that they do have the rights to. The same issue may be present in third party authentication/access control plugins for Mosquitto.	mosquitto 1.4.8	Patch #3

CVE	Description	Package	Fixed In
CVE-2016-6480	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/ commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a "double fetch" vulnerability.	linux-ls1_4.1	Patch #3
CVE-2015-5156	The virtnet_probe function in drivers/net/ virtio_net.c in the Linux kernel before 4.2 attempts to support a FRAGLIST feature without proper memory allocation, which allows guest OS users to cause a denial of service (buffer overflow and memory corruption) via a crafted sequence of fragmented packets.	linux-qoriq_4.1	Patch #3
CVE-2015-5257	drivers/usb/serial/whiteheat.c in the Linux kernel before 4.2.4 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) or possibly have unspecified other impact via a crafted USB device. NOTE: this ID was incorrectly used for an Apache Cordova issue that has the correct ID of CVE-2015-8320.	linux-qoriq_4.1	Patch #3
CVE-2016-0728	The join_session_keyring function in security/ keys/process_keys.c 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 keyctl commands.	linux-qoriq_4.1	Patch #3
CVE-2016-2384	Double free vulnerability in the snd_usbmidi_create function in sound/usb/ midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.	linux-qoriq_4.1	Patch #3
CVE-2016-3136	The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device without two interrupt-in endpoint descriptors.	linux-qoriq_4.1	Patch #3

CVE	Description	Package	Fixed In
CVE-2016-3156	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.	linux-qoriq_4.1	Patch #3
CVE-2016-4951	The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation.	linux-qoriq_4.1	Patch #3
CVE-2016-5829	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call.	linux-qoriq_4.1	Patch #3
CVE-2016-9754	The ring_buffer_resize function in kernel/trace/ring_buffer.c in the profiling subsystem in the Linux kernel before 4.6.1 mishandles certain integer calculations, which allows local users to gain privileges by writing to the / sys/kernel/debug/tracing/buffer_size_kb file.	linux-qoriq_4.1	Patch #3
CVE-2017-1000365	The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/ RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-ls1_4.1 linux-qoriq_4.1 linux-mel_4.1.37-mx6q	Patch #3
CVE-2016-9840	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.	zlib 1.2.8	Patch #2

CVE	Description	Package	Fixed In
CVE-2016-9841	inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.	zlib 1.2.8	Patch #2
CVE-2016-9843	The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.	zlib 1.2.8	Patch #2
CVE-2016-9842	The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers.	zlib 1.2.8	Patch #2
CVE-2016-9318	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.	libxml2 2.9.4	Patch #2
CVE-2016-10087	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into a png structure, removing the text, and then adding another text chunk to the structure.	libpng 1.6.24	Patch #2
CVE-2017-5969	CVE_links.txt cve.txt CVE.txt des.txt fix.txt NonCVE.txt out_abcd.txt out_abc.txt out_final.txt out_links.txt out.xlsx pack.txt trial.sh xcl.py DISPUTED CVE_links.txt cve.txt CVE.txt des.txt fix.txt NonCVE.txt out_abcd.txt out_abc.txt out_final.txt out_links.txt out.xlsx pack.txt trial.sh xcl.py libxml2 2.9.4, when used in recover mode, allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted XML document. NOTE: The maintainer states "I would disagree of a CVE with the Recover parsing option which should only be used for manual recovery at least for XML parser."	libxml2 2.9.4	Patch #2

CVE	Description	Package	Fixed In
CVE-2017-9047	A buffer overflow was discovered in libxml2 20904-GITv2.9.4-16-g0741801. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable len is assigned strlen(buf). If the content->type is XML_ELEMENT_CONTENT_ELEMENT, then (i) the content->prefix is appended to buf (if it actually fits) whereupon (ii) content->name is written to the buffer. However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffer length strlen(buf). This allows us to write about "size" many bytes beyond the allocated memory. This vulnerability causes programs that use libxml2, such as PHP, to crash.	libxml2 2.9.4	Patch #2
CVE-2017-9049	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictComputeFastKey function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for libxml2 Bug 759398.	libxml2 2.9.4	Patch #2
CVE-2017-7960	The cr_input_new_from_uri function in cr-input.c in libcroco 0.6.11 and 0.6.12 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted CSS file.	libcroco 0.6.11	Patch #2

CVE	Description	Package	Fixed In
CVE-2017-7961	CVE_links.txt cve.txt CVE.txt des.txt fix.txt NonCVE.txt out_abcd.txt out_abc.txt out_final.txt out_links.txt out.xlsx pack.txt trial.sh xcl.py DISPUTED CVE_links.txt cve.txt CVE.txt des.txt fix.txt NonCVE.txt out_abcd.txt out_abc.txt out_final.txt out_links.txt out.xlsx pack.txt trial.sh xcl.py The cr_tknzr_parse_rgb function in cr-tknzr.c in libcroco 0.6.11 and 0.6.12 has an "outside the range of representable values of type long" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted CSS file. NOTE: third-party analysis reports "This is not a security issue in my view. The conversion surely is truncating the double into a long value, but there is no impact as the value is one of the RGB components."	libcroco 0.6.11	Patch #2
CVE-2017-3731	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.	openssl 1.0.2j	Patch #2
CVE-2016-9082	Integer overflow in the write_png function in cairo 1.14.6 allows remote attackers to cause a denial of service (invalid pointer dereference) via a large svg file.	cairo 1.14.6	Patch #1
CVE-2017-5334	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.	gnutls 3.5.3	Patch #1

CVE	Description	Package	Fixed In
CVE-2017-5335	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.	gnutls 3.5.3	Patch #1
CVE-2017-5336	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.	gnutls 3.5.3	Patch #1
CVE-2017-5337	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.	gnutls 3.5.3	Patch #1
CVE-2016-8687	Stack-based buffer overflow in the safe_fprintf function in tar/util.c in libarchive 3.2.1 allows remote attackers to cause a denial of service via a crafted non-printable multibyte character in a filename.	libarchive 3.2.1	Patch #1
CVE-2016-8688	The mtree bidder in libarchive 3.2.1 does not keep track of line sizes when extending the read-ahead, which allows remote attackers to cause a denial of service (crash) via a crafted file, which triggers an invalid read in the (1) detect_form or (2) bid_entry function in libarchive/archive_read_support_format_mtree.c.	libarchive 3.2.1	Patch #1
CVE-2016-8689	The read_Header function in archive_read_support_format_7zip.c in libarchive 3.2.1 allows remote attackers to cause a denial of service (out-of-bounds read) via multiple EmptyStream attributes in a header in a 7zip archive.	libarchive 3.2.1	Patch #1
CVE-2014-9913	Buffer overflow in the list_files function in list.c in Info-Zip UnZip 6.0 allows remote attackers to cause a denial of service (crash) via vectors related to the compression method.	unzip 6.0	Patch #1

CVE	Description	Package	Fixed In
CVE-2016-9844	Buffer overflow in the zi_short function in zipinfo.c in Info-Zip UnZip 6.0 allows remote attackers to cause a denial of service (crash) via a large compression method value in the central directory file header.	unzip 6.0	Patch #1
CVE-2016-5180	Heap-based buffer overflow in the ares_create_query function in c-ares 1.x before 1.12.0 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly execute arbitrary code via a hostname with an escaped trailing dot.	c-ares 1.10.0	Patch #1
CVE-2009-3994	Stack-based buffer overflow in the GetUID function in src-IL/src/il_dicom.c in DevIL 1.7.8 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted DICOM file.	devil 1.7.8	Patch #1
CVE-2016-9941	Heap-based buffer overflow in rfbproto.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message containing a subrectangle outside of the client drawing area.	libvncserver 0.9.10	Patch #1
CVE-2016-9942	Heap-based buffer overflow in ultra.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message with the Ultra type tile, such that the LZO payload decompressed length exceeds what is specified by the tile dimensions.	libvncserver 0.9.10	Patch #1
CVE-2016-5407	The (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXv before 1.0.11 allow remote X servers to trigger out-of-bounds memory access operations via vectors involving length specifications in received data.	libxv 1.0.10	Patch #1
CVE-2016-7953	Buffer underflow in X.org libXvMC before 1.0.10 allows remote X servers to have unspecified impact via an empty string.	libxvmc 1.0.9	Patch #1

CVE	Description	Package	Fixed In
CVE-2016-6252	Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap.	shadow 4.2.1	Patch #1
CVE-2016-6321	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to bypass an intended protection mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka POINTYFEATHER.	tar 1.29	Patch #1
CVE-2015-8956	The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket.	linux-qoriq_4.1 linux-ls1_4.1	Patch #1
CVE-2017-7273	The cp_report_fixup function in drivers/hid/hid-cypress.c in the Linux kernel 4.x before 4.9.4 allows physically proximate attackers to cause a denial of service (integer underflow) or possibly have unspecified other impact via a crafted HID report.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-ls1_4.1 linux-xlnx_4.4-xilinx	Patch #1
CVE-2017-6074	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.	linux-altera-ltsi_4.1.22 linux-yocto_4.1.33 linux-qoriq_4.1 linux-mel_4.1.37-mx6q linux-ls1_4.1 linux-xlnx_4.4-xilinx	Patch #1

Global Customer Support and Success

A support contract with Mentor, a Siemens Business, is a valuable investment in your organization’s success. With a support contract, you have 24/7 access to the comprehensive and personalized Support Center portal.

Support Center features an extensive knowledge base to quickly troubleshoot issues by product and version. You can also download the latest releases, access the most up-to-date documentation, and submit a support case through a streamlined process.

`https://support.sw.siemens.com`

If your site is under a current support contract, but you do not have a Support Center login, register here:

`https://support.sw.siemens.com/register`

Mentor Graphics
A Siemens Business

End-User License Agreement with Embedded Software Supplement

Use of software (including any updates) and/or hardware is subject to the End-User License Agreement together with the Embedded Software Supplement Terms. You can view and print a copy of this agreement at:

mentor.com/embeddedeula