CVE Report

CVE ID: CVE-2011-3374
Description: It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the maste
Mitigation: No fix available

CVE ID: TEMP-0841856-B18BAF
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2016-2781
Description: chroot in GNU coreutils, when used with --userspec, allows local users to escape to the paren
Mitigation: No fix available

CVE ID: CVE-2017-18018
Description: In GNU Coreutils through 8.29, chown-core.c in chown and chgrp does not prevent replaceme
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2024-11053
Description: When asked to both use a `.netrc` file for credentials and to follow HTTP■redirects, curl could
Mitigation: No fix available

CVE ID: CVE-2024-9681
Description: When curl is asked to use HSTS, the expiry time for a subdomain might■overwrite a parent d
Mitigation: No fix available

CVE ID: CVE-2024-2379
Description: libcurl skips the certificate verification for a QUIC connection under certain conditions, when b
Mitigation: No fix available

CVE ID: CVE-2022-3219
Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key v
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2024-52006
Description: Git is a fast, scalable, distributed revision control system with an unusually rich command set
Mitigation: No fix available

CVE ID: CVE-2018-1000021
Description: GIT version 2.15.1 and earlier contains a Input Validation Error vulnerability in Client that can
Mitigation: No fix available

CVE ID: CVE-2022-24975
Description: The --mirror documentation for Git through 2.35.1 does not mention the availability of deleted
Mitigation: No fix available

CVE ID: CVE-2024-50349
Description: Git is a fast, scalable, distributed revision control system with an unusually rich command set
Mitigation: No fix available

CVE ID: CVE-2024-52006
Description: Git is a fast, scalable, distributed revision control system with an unusually rich command set
Mitigation: No fix available

CVE ID: CVE-2018-1000021
Description: GIT version 2.15.1 and earlier contains a Input Validation Error vulnerability in Client that can
Mitigation: No fix available

CVE ID: CVE-2022-24975

Description: The --mirror documentation for Git through 2.35.1 does not mention the availability of deleted

Mitigation: No fix available

CVE ID: CVE-2024-50349

Description: Git is a fast, scalable, distributed revision control system with an unusually rich command set

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219

Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key

Mitigation: No fix available

CVE ID: CVE-2022-3219
Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key v
Mitigation: No fix available

CVE ID: CVE-2022-3219
Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key v
Mitigation: No fix available

CVE ID: CVE-2022-3219
Description: GnuPG can be made to spin on a relatively small input by (for example) crafting a public key v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2023-6879
Description: Increasing the resolution of video frames, while performing a multi-threaded encode, can resu
Mitigation: No fix available

CVE ID: CVE-2023-39616
Description: AOMedia v3.0.0 to v3.5.0 was discovered to contain an invalid read memory access via the co
Mitigation: No fix available

CVE ID: CVE-2011-3374
Description: It was found that apt-key in apt, all versions, do not correctly validate gpg keys with the maste
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2023-44431
Description: BlueZ Audio Profile AVRCP Stack-based Buffer Overflow Remote Code Execution Vulnerabili
Mitigation: No fix available

CVE ID: CVE-2023-51596
Description: BlueZ Phone Book Access Profile Heap-based Buffer Overflow Remote Code Execution Vuln
Mitigation: No fix available

CVE ID: CVE-2023-51580
Description: BlueZ Audio Profile AVRCP avrcp_parse_attribute_list Out-Of-Bounds Read Information Disc
Mitigation: No fix available

CVE ID: CVE-2023-51589
Description: BlueZ Audio Profile AVRCP parse_media_element Out-Of-Bounds Read Information Disclosu
Mitigation: No fix available

CVE ID: CVE-2023-51592
Description: BlueZ Audio Profile AVRCP parse_media_folder Out-Of-Bounds Read Information Disclosure
Mitigation: No fix available

CVE ID: CVE-2016-9797
Description: In BlueZ 5.42, a buffer over-read was observed in "l2cap_dump" function in "tools/parser/l2ca
Mitigation: No fix available

CVE ID: CVE-2016-9798
Description: In BlueZ 5.42, a use-after-free was identified in "conf_opt" function in "tools/parser/l2cap.c" so
Mitigation: No fix available

CVE ID: CVE-2016-9799
Description: In BlueZ 5.42, a buffer overflow was observed in "pklg_read_hci" function in "btsnoop.c" sourc
Mitigation: No fix available

CVE ID: CVE-2016-9800
Description: In BlueZ 5.42, a buffer overflow was observed in "pin_code_reply_dump" function in "tools/pa
Mitigation: No fix available

CVE ID: CVE-2016-9801
Description: In BlueZ 5.42, a buffer overflow was observed in "set_ext_ctrl" function in "tools/parser/l2cap.
Mitigation: No fix available

CVE ID: CVE-2016-9802
Description: In BlueZ 5.42, a buffer over-read was identified in "l2cap_packet" function in "monitor/packet.
Mitigation: No fix available

CVE ID: CVE-2016-9803
Description: In BlueZ 5.42, an out-of-bounds read was observed in "le_meta_ev_dump" function in "tools/p
Mitigation: No fix available

CVE ID: CVE-2016-9804
Description: In BlueZ 5.42, a buffer overflow was observed in "commands_dump" function in "tools/parser/
Mitigation: No fix available

CVE ID: CVE-2016-9917
Description: In BlueZ 5.42, a buffer overflow was observed in "read_n" function in "tools/hcidump.c" source
Mitigation: No fix available

CVE ID: CVE-2016-9918
Description: In BlueZ 5.42, an out-of-bounds read was identified in "packet_hexdump" function in "monitor/
Mitigation: No fix available

CVE ID: CVE-2023-51594
Description: BlueZ OBEX Library Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerabi
Mitigation: No fix available

CVE ID: CVE-2023-44431
Description: BlueZ Audio Profile AVRCP Stack-based Buffer Overflow Remote Code Execution Vulnerabili
Mitigation: No fix available

CVE ID: CVE-2023-51596
Description: BlueZ Phone Book Access Profile Heap-based Buffer Overflow Remote Code Execution Vuln
Mitigation: No fix available

CVE ID: CVE-2023-51580
Description: BlueZ Audio Profile AVRCP avrcp_parse_attribute_list Out-Of-Bounds Read Information Disc
Mitigation: No fix available

CVE ID: CVE-2023-51589
Description: BlueZ Audio Profile AVRCP parse_media_element Out-Of-Bounds Read Information Disclosu
Mitigation: No fix available

CVE ID: CVE-2023-51592
Description: BlueZ Audio Profile AVRCP parse_media_folder Out-Of-Bounds Read Information Disclosure
Mitigation: No fix available

CVE ID: CVE-2016-9797
Description: In BlueZ 5.42, a buffer over-read was observed in "l2cap_dump" function in "tools/parser/l2ca
Mitigation: No fix available

CVE ID: CVE-2016-9798
Description: In BlueZ 5.42, a use-after-free was identified in "conf_opt" function in "tools/parser/l2cap.c" so
Mitigation: No fix available

CVE ID: CVE-2016-9799
Description: In BlueZ 5.42, a buffer overflow was observed in "pklg_read_hci" function in "btsnoop.c" sourc
Mitigation: No fix available

CVE ID: CVE-2016-9800
Description: In BlueZ 5.42, a buffer overflow was observed in "pin_code_reply_dump" function in "tools/pa
Mitigation: No fix available

CVE ID: CVE-2016-9801
Description: In BlueZ 5.42, a buffer overflow was observed in "set_ext_ctrl" function in "tools/parser/l2cap.
Mitigation: No fix available

CVE ID: CVE-2016-9802
Description: In BlueZ 5.42, a buffer over-read was identified in "l2cap_packet" function in "monitor/packet.
Mitigation: No fix available

CVE ID: CVE-2016-9803
Description: In BlueZ 5.42, an out-of-bounds read was observed in "le_meta_ev_dump" function in "tools/p
Mitigation: No fix available

CVE ID: CVE-2016-9804
Description: In BlueZ 5.42, a buffer overflow was observed in "commands_dump" function in "tools/parser/
Mitigation: No fix available

CVE ID: CVE-2016-9917
Description: In BlueZ 5.42, a buffer overflow was observed in "read_n" function in "tools/hcidump.c" source
Mitigation: No fix available

CVE ID: CVE-2016-9918
Description: In BlueZ 5.42, an out-of-bounds read was identified in "packet_hexdump" function in "monitor/
Mitigation: No fix available

CVE ID: CVE-2023-51594
Description: BlueZ OBEX Library Out-Of-Bounds Read Information Disclosure Vulnerability. This vulnerabi
Mitigation: No fix available

CVE ID: CVE-2010-4756
Description: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated
Mitigation: No fix available

CVE ID: CVE-2018-20796
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2019-1010022
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack
Mitigation: No fix available

CVE ID: CVE-2019-1010023
Description: GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. Th
Mitigation: No fix available

CVE ID: CVE-2019-1010024
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR
Mitigation: No fix available

CVE ID: CVE-2019-1010025
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the hea
Mitigation: No fix available

CVE ID: CVE-2019-9192
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2010-4756
Description: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated
Mitigation: No fix available

CVE ID: CVE-2018-20796
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2019-1010022
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack
Mitigation: No fix available

CVE ID: CVE-2019-1010023
Description: GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. Th
Mitigation: No fix available

CVE ID: CVE-2019-1010024
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR
Mitigation: No fix available

CVE ID: CVE-2019-1010025
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the hea
Mitigation: No fix available

CVE ID: CVE-2019-9192
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2010-4756
Description: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated
Mitigation: No fix available

CVE ID: CVE-2018-20796
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2019-1010022
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack
Mitigation: No fix available

CVE ID: CVE-2019-1010023
Description: GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. Th
Mitigation: No fix available

CVE ID: CVE-2019-1010024
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR
Mitigation: No fix available

CVE ID: CVE-2019-1010025
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the hea
Mitigation: No fix available

CVE ID: CVE-2019-9192
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2010-4756
Description: The glob implementation in the GNU C Library (aka glibc or libc6) allows remote authenticated
Mitigation: No fix available

CVE ID: CVE-2018-20796
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2019-1010022
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass stack
Mitigation: No fix available

CVE ID: CVE-2019-1010023
Description: GNU Libc current is affected by: Re-mapping current loaded library with malicious ELF file. Th
Mitigation: No fix available

CVE ID: CVE-2019-1010024
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may bypass ASLR
Mitigation: No fix available

CVE ID: CVE-2019-1010025
Description: GNU Libc current is affected by: Mitigation bypass. The impact is: Attacker may guess the hea
Mitigation: No fix available

CVE ID: CVE-2019-9192
Description: In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/r
Mitigation: No fix available

CVE ID: CVE-2017-7475
Description: Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyp
Mitigation: No fix available

CVE ID: CVE-2018-18064
Description: cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted
Mitigation: No fix available

CVE ID: CVE-2019-6461
Description: An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_
Mitigation: No fix available

CVE ID: CVE-2019-6462
Description: An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_no
Mitigation: No fix available

CVE ID: CVE-2017-7475
Description: Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyp
Mitigation: No fix available

CVE ID: CVE-2018-18064
Description: cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted
Mitigation: No fix available

CVE ID: CVE-2019-6461
Description: An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_
Mitigation: No fix available

CVE ID: CVE-2019-6462
Description: An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_no
Mitigation: No fix available

CVE ID: CVE-2017-7475
Description: Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyp
Mitigation: No fix available

CVE ID: CVE-2018-18064
Description: cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted
Mitigation: No fix available

CVE ID: CVE-2019-6461
Description: An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_
Mitigation: No fix available

CVE ID: CVE-2019-6462
Description: An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_no
Mitigation: No fix available

CVE ID: CVE-2017-7475
Description: Cairo version 1.15.4 is vulnerable to a NULL pointer dereference related to the FT_Load_Glyp
Mitigation: No fix available

CVE ID: CVE-2018-18064
Description: cairo through 1.15.14 has an out-of-bounds stack-memory write during processing of a crafted
Mitigation: No fix available

CVE ID: CVE-2019-6461
Description: An issue was discovered in cairo 1.16.0. There is an assertion problem in the function _cairo_
Mitigation: No fix available

CVE ID: CVE-2019-6462
Description: An issue was discovered in cairo 1.16.0. There is an infinite loop in the function _arc_error_no
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2024-11053
Description: When asked to both use a `.netrc` file for credentials and to follow HTTP■redirects, curl could
Mitigation: No fix available

CVE ID: CVE-2024-9681
Description: When curl is asked to use HSTS, the expiry time for a subdomain might■overwrite a parent d
Mitigation: No fix available

CVE ID: CVE-2024-2379
Description: libcurl skips the certificate verification for a QUIC connection under certain conditions, when b
Mitigation: No fix available

CVE ID: CVE-2024-11053
Description: When asked to both use a `.netrc` file for credentials and to follow HTTP■redirects, curl could
Mitigation: No fix available

CVE ID: CVE-2024-9681
Description: When curl is asked to use HSTS, the expiry time for a subdomain might■overwrite a parent d
Mitigation: No fix available

CVE ID: CVE-2024-2379
Description: libcurl skips the certificate verification for a QUIC connection under certain conditions, when b
Mitigation: No fix available

CVE ID: CVE-2024-11053
Description: When asked to both use a `.netrc` file for credentials and to follow HTTP■redirects, curl could
Mitigation: No fix available

CVE ID: CVE-2024-9681
Description: When curl is asked to use HSTS, the expiry time for a subdomain might■overwrite a parent d
Mitigation: No fix available

CVE ID: CVE-2024-2379
Description: libcurl skips the certificate verification for a QUIC connection under certain conditions, when b
Mitigation: No fix available

CVE ID: CVE-2023-32570
Description: VideoLAN dav1d before 1.2.0 has a thread_task.c race condition that can lead to an applicatio
Mitigation: No fix available

CVE ID: CVE-2023-51792
Description: Buffer Overflow vulnerability in libde265 v1.0.12 allows a local attacker to cause a denial of se
Mitigation: No fix available

CVE ID: CVE-2024-38949

Description: Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attackers to crash the applicatio

Mitigation: No fix available

CVE ID: CVE-2024-38950

Description: Heap Buffer Overflow vulnerability in Libde265 v1.0.15 allows attackers to crash the applicatio

Mitigation: No fix available

CVE ID: CVE-2021-46310

Description: An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a de

Mitigation: No fix available

CVE ID: CVE-2021-46312

Description: An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cau

Mitigation: No fix available

CVE ID: CVE-2021-46310

Description: An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a de

Mitigation: No fix available

CVE ID: CVE-2021-46312

Description: An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cau

Mitigation: No fix available

CVE ID: CVE-2021-46310

Description: An issue was discovered IW44Image.cpp in djvulibre 3.5.28 in allows attackers to cause a de

Mitigation: No fix available

CVE ID: CVE-2021-46312

Description: An issue was discovered IW44EncodeCodec.cpp in djvulibre 3.5.28 in allows attackers to cau

Mitigation: No fix available

CVE ID: CVE-2024-25260

Description: elfutils v0.189 was discovered to contain a NULL pointer dereference via the handle_verdef()

Mitigation: No fix available

CVE ID: CVE-2023-52425
Description: libexpat through 2.5.0 allows a denial of service (resource consumption) because many full re
Mitigation: No fix available

CVE ID: CVE-2024-50602
Description: An issue was discovered in libexpat before 2.6.4. There is a crash within the XML_ResumePa
Mitigation: No fix available

CVE ID: CVE-2023-52426
Description: libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DTD is undefined at con
Mitigation: No fix available

CVE ID: CVE-2024-28757
Description: libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of ex
Mitigation: No fix available

CVE ID: CVE-2023-52425
Description: libexpat through 2.5.0 allows a denial of service (resource consumption) because many full re
Mitigation: No fix available

CVE ID: CVE-2024-50602
Description: An issue was discovered in libexpat before 2.6.4. There is a crash within the XML_ResumePa
Mitigation: No fix available

CVE ID: CVE-2023-52426
Description: libexpat through 2.5.0 allows recursive XML Entity Expansion if XML_DTD is undefined at con
Mitigation: No fix available

CVE ID: CVE-2024-28757
Description: libexpat through 2.6.1 allows an XML Entity Expansion attack when there is isolated use of ex
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2024-2236
Description: A timing-based side-channel flaw was found in libgcrypt's RSA implementation. This issue ma
Mitigation: No fix available

CVE ID: CVE-2018-6829
Description: cipher/elgamal.c in Libgcrypt through 1.8.2, when used to encrypt messages directly, improper
Mitigation: No fix available

CVE ID: CVE-2012-0039
Description: GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without
Mitigation: No fix available

CVE ID: CVE-2012-0039
Description: GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without
Mitigation: No fix available

CVE ID: CVE-2012-0039
Description: GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without
Mitigation: No fix available

CVE ID: CVE-2012-0039
Description: GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without
Mitigation: No fix available

CVE ID: CVE-2012-0039
Description: GLib 2.31.8 and earlier, when the g_str_hash function is used, computes hash values without
Mitigation: No fix available

CVE ID: CVE-2011-3389
Description: The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Intern
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2017-13716
Description: The C++ symbol demangler routine in cplus-dem.c in libiberty, as distributed in GNU Binutils 2
Mitigation: No fix available

CVE ID: CVE-2018-20673
Description: The demangle_template function in cplus-dem.c in GNU libiberty, as distributed in GNU Binuti
Mitigation: No fix available

CVE ID: CVE-2018-20712
Description: A heap-based buffer over-read exists in the function d_expression_1 in cp-demangle.c in GNU
Mitigation: No fix available

CVE ID: CVE-2018-9996
Description: An issue was discovered in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30.
Mitigation: No fix available

CVE ID: CVE-2021-32256
Description: An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.36. It is a stack-ove
Mitigation: No fix available

CVE ID: CVE-2023-1972
Description: A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf
Mitigation: No fix available

CVE ID: CVE-2024-53589
Description: GNU objdump 2.43 is vulnerable to Buffer Overflow in the BFD (Binary File Descriptor) library
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2023-25193
Description: hb-ot-layout-gsubgpos.hh in HarfBuzz through 6.0.0 allows attackers to trigger O(n^2) growth
Mitigation: No fix available

CVE ID: CVE-2023-49463
Description: libheif v1.17.5 was discovered to contain a segmentation violation via the function find_exif_ta
Mitigation: No fix available

CVE ID: CVE-2024-25269
Description: libheif <= 1.17.6 contains a memory leak in the function JpegEncoder::Encode. This flaw allow
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2020-36325
Description: An issue was discovered in Jansson through 2.13.1. Due to a parsing error in json_loads, ther
Mitigation: No fix available

CVE ID: CVE-2017-9937
Description: In LibTIFF 4.0.8, there is a memory malloc failure in tif_jbig.c. A crafted TIFF document can le
Mitigation: No fix available

CVE ID: CVE-2017-9937
Description: In LibTIFF 4.0.8, there is a memory malloc failure in tif_jbig.c. A crafted TIFF document can le
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2024-26462
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/kdc/ndr.c.
Mitigation: No fix available

CVE ID: CVE-2018-5709
Description: An issue was discovered in MIT Kerberos 5 (aka krb5) through 1.16. There is a variable "dber
Mitigation: No fix available

CVE ID: CVE-2024-26458
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak in /krb5/src/lib/rpc/pmap_rmt.c.
Mitigation: No fix available

CVE ID: CVE-2024-26461
Description: Kerberos 5 (aka krb5) 1.21.2 contains a memory leak vulnerability in /krb5/src/lib/gssapi/krb5/
Mitigation: No fix available

CVE ID: CVE-2023-2953
Description: A vulnerability was found in openldap. This security flaw causes a null pointer dereference in l
Mitigation: No fix available

CVE ID: CVE-2015-3276
Description: The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly pa
Mitigation: No fix available

CVE ID: CVE-2017-14159
Description: slapd in OpenLDAP 2.4.45 and earlier creates a PID file after dropping privileges to a non-roo
Mitigation: No fix available

CVE ID: CVE-2017-17740
Description: contrib/slapd-modules/nops/nops.c in OpenLDAP through 2.4.45, when both the nops module
Mitigation: No fix available

CVE ID: CVE-2020-15719
Description: libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the th
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2005-0406
Description: A design flaw in image processing software that modifies JPEG images might not modify the c
Mitigation: No fix available

CVE ID: CVE-2008-3134
Description: Multiple unspecified vulnerabilities in GraphicsMagick before 1.2.4 allow remote attackers to c
Mitigation: No fix available

CVE ID: CVE-2016-8678
Description: The IsPixelMonochrome function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3.0 allo
Mitigation: No fix available

CVE ID: CVE-2017-11754
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-11755
Description: The WritePICONImage function in coders/xpm.c in ImageMagick 7.0.6-4 allows remote attack
Mitigation: No fix available

CVE ID: CVE-2017-7275
Description: The ReadPCXImage function in coders/pcx.c in ImageMagick 7.0.4.9 allows remote attackers
Mitigation: No fix available

CVE ID: CVE-2018-15607
Description: In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x3
Mitigation: No fix available

CVE ID: CVE-2021-20311
Description: A flaw was found in ImageMagick in versions before 7.0.11, where a division by zero in sRGB
Mitigation: No fix available

CVE ID: CVE-2023-34152
Description: A vulnerability was found in ImageMagick. This security flaw cause a remote code execution v
Mitigation: No fix available

CVE ID: CVE-2024-21096
Description: Vulnerability in the MySQL Server product of Oracle MySQL (component: Client: mysqldump)
Mitigation: No fix available

CVE ID: CVE-2024-21096

Description: Vulnerability in the MySQL Server product of Oracle MySQL (component: Client: mysqldump)

Mitigation: No fix available

CVE ID: CVE-2024-21096

Description: Vulnerability in the MySQL Server product of Oracle MySQL (component: Client: mysqldump)

Mitigation: No fix available

CVE ID: CVE-2022-0563

Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.

Mitigation: No fix available

CVE ID: CVE-2022-0563

Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.

Mitigation: No fix available

CVE ID: CVE-2023-50495

Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n

Mitigation: No fix available

CVE ID: CVE-2023-50495

Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n

Mitigation: No fix available

CVE ID: CVE-2023-50495

Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n

Mitigation: No fix available

CVE ID: CVE-2023-50495

Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n

Mitigation: No fix available

CVE ID: CVE-2023-50495

Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n

Mitigation: No fix available

CVE ID: CVE-2023-5841
Description: Due to a failure in validating the number of scanline samples of a OpenEXR file containing de
Mitigation: No fix available

CVE ID: CVE-2017-14988
Description: Header::readfrom in IlmImf/ImfHeader.cpp in OpenEXR 2.2.0 allows remote attackers to caus
Mitigation: No fix available

CVE ID: CVE-2024-31047
Description: An issue in Academy Software Foundation openexr v.3.2.3 and before allows a local attacker
Mitigation: No fix available

CVE ID: CVE-2023-5841
Description: Due to a failure in validating the number of scanline samples of a OpenEXR file containing de
Mitigation: No fix available

CVE ID: CVE-2017-14988
Description: Header::readfrom in IlmImf/ImfHeader.cpp in OpenEXR 2.2.0 allows remote attackers to caus
Mitigation: No fix available

CVE ID: CVE-2024-31047
Description: An issue in Academy Software Foundation openexr v.3.2.3 and before allows a local attacker
Mitigation: No fix available

CVE ID: CVE-2021-3575
Description: A heap-based buffer overflow was found in openjpeg in color.c:379:42 in sycc420_to_rgb whe
Mitigation: No fix available

CVE ID: CVE-2023-39327
Description: A flaw was found in OpenJPEG. Maliciously constructed pictures can cause the program to en
Mitigation: No fix available

CVE ID: CVE-2023-39328
Description: A vulnerability was found in OpenJPEG similar to CVE-2019-6988. This flaw allows an attacke
Mitigation: No fix available

CVE ID: CVE-2023-39329
Description: A flaw was found in OpenJPEG. A resource exhaustion can occur in the opj_t1_decode_cblks
Mitigation: No fix available

CVE ID: CVE-2024-56826
Description: A flaw was found in the OpenJPEG project. A heap buffer overflow condition may be triggered
Mitigation: No fix available

CVE ID: CVE-2024-56827
Description: A flaw was found in the OpenJPEG project. A heap buffer overflow condition may be triggered
Mitigation: No fix available

CVE ID: CVE-2016-10505
Description: NULL pointer dereference vulnerabilities in the imagetopnm function in convert.c, sycc444_to_
Mitigation: No fix available

CVE ID: CVE-2016-9113
Description: There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJP
Mitigation: No fix available

CVE ID: CVE-2016-9114
Description: There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG
Mitigation: No fix available

CVE ID: CVE-2016-9115
Description: Heap Buffer Over-read in function imagetotga of convert.c(jp2):942 in OpenJPEG 2.1.2. Impa
Mitigation: No fix available

CVE ID: CVE-2016-9116
Description: NULL Pointer Access in function imagetopnm of convert.c:2226(jp2) in OpenJPEG 2.1.2. Impa
Mitigation: No fix available

CVE ID: CVE-2016-9117
Description: NULL Pointer Access in function imagetopnm of convert.c(jp2):1289 in OpenJPEG 2.1.2. Impa
Mitigation: No fix available

CVE ID: CVE-2016-9580
Description: An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting i
Mitigation: No fix available

CVE ID: CVE-2016-9581
Description: An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C
Mitigation: No fix available

CVE ID: CVE-2017-17479
Description: In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtoimage function
Mitigation: No fix available

CVE ID: CVE-2018-16375
Description: An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and hea
Mitigation: No fix available

CVE ID: CVE-2018-16376
Description: An issue was discovered in OpenJPEG 2.3.0. A heap-based buffer overflow was discovered i
Mitigation: No fix available

CVE ID: CVE-2018-20846
Description: Out-of-bounds accesses in the functions pi_next_lrcp, pi_next_rlcp, pi_next_rpcl, pi_next_pcrl
Mitigation: No fix available

CVE ID: CVE-2019-6988
Description: An issue was discovered in OpenJPEG 2.3.0. It allows remote attackers to cause a denial of s
Mitigation: No fix available

CVE ID: CVE-2021-3575
Description: A heap-based buffer overflow was found in openjpeg in color.c:379:42 in sycc420_to_rgb whe
Mitigation: No fix available

CVE ID: CVE-2023-39327
Description: A flaw was found in OpenJPEG. Maliciously constructed pictures can cause the program to en
Mitigation: No fix available

CVE ID: CVE-2023-39328
Description: A vulnerability was found in OpenJPEG similar to CVE-2019-6988. This flaw allows an attacke
Mitigation: No fix available

CVE ID: CVE-2023-39329
Description: A flaw was found in OpenJPEG. A resource exhaustion can occur in the opj_t1_decode_cblks
Mitigation: No fix available

CVE ID: CVE-2024-56826
Description: A flaw was found in the OpenJPEG project. A heap buffer overflow condition may be triggered
Mitigation: No fix available

CVE ID: CVE-2024-56827
Description: A flaw was found in the OpenJPEG project. A heap buffer overflow condition may be triggered
Mitigation: No fix available

CVE ID: CVE-2016-10505
Description: NULL pointer dereference vulnerabilities in the imagetopnm function in convert.c, sycc444_to_
Mitigation: No fix available

CVE ID: CVE-2016-9113
Description: There is a NULL pointer dereference in function imagetobmp of convertbmp.c:980 of OpenJP
Mitigation: No fix available

CVE ID: CVE-2016-9114
Description: There is a NULL Pointer Access in function imagetopnm of convert.c:1943(jp2) of OpenJPEG
Mitigation: No fix available

CVE ID: CVE-2016-9115
Description: Heap Buffer Over-read in function imagetotga of convert.c(jp2):942 in OpenJPEG 2.1.2. Impa
Mitigation: No fix available

CVE ID: CVE-2016-9116
Description: NULL Pointer Access in function imagetopnm of convert.c:2226(jp2) in OpenJPEG 2.1.2. Impa
Mitigation: No fix available

CVE ID: CVE-2016-9117
Description: NULL Pointer Access in function imagetopnm of convert.c(jp2):1289 in OpenJPEG 2.1.2. Impa
Mitigation: No fix available

CVE ID: CVE-2016-9580
Description: An integer overflow vulnerability was found in tiftoimage function in openjpeg 2.1.2, resulting i
Mitigation: No fix available

CVE ID: CVE-2016-9581
Description: An infinite loop vulnerability in tiftoimage that results in heap buffer overflow in convert_32s_C
Mitigation: No fix available

CVE ID: CVE-2017-17479
Description: In OpenJPEG 2.3.0, a stack-based buffer overflow was discovered in the pgxtoimage function
Mitigation: No fix available

CVE ID: CVE-2018-16375
Description: An issue was discovered in OpenJPEG 2.3.0. Missing checks for header_info.height and head
Mitigation: No fix available

CVE ID: CVE-2018-16376
Description: An issue was discovered in OpenJPEG 2.3.0. A heap-based buffer overflow was discovered i
Mitigation: No fix available

CVE ID: CVE-2018-20846
Description: Out-of-bounds accesses in the functions pi_next_lrcp, pi_next_rlcp, pi_next_rpcl, pi_next_pcrl
Mitigation: No fix available

CVE ID: CVE-2019-6988
Description: An issue was discovered in OpenJPEG 2.3.0. It allows remote attackers to cause a denial of s
Mitigation: No fix available

CVE ID: CVE-2024-10041
Description: A vulnerability was found in PAM. The secret information is stored in memory, where the attac
Mitigation: No fix available

CVE ID: CVE-2024-22365

Description: linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked

Mitigation: No fix available

CVE ID: CVE-2024-10041

Description: A vulnerability was found in PAM. The secret information is stored in memory, where the attac

Mitigation: No fix available

CVE ID: CVE-2024-22365

Description: linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked

Mitigation: No fix available

CVE ID: CVE-2024-10041

Description: A vulnerability was found in PAM. The secret information is stored in memory, where the attac

Mitigation: No fix available

CVE ID: CVE-2024-22365

Description: linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked

Mitigation: No fix available

CVE ID: CVE-2024-10041

Description: A vulnerability was found in PAM. The secret information is stored in memory, where the attac

Mitigation: No fix available

CVE ID: CVE-2024-22365

Description: linux-pam (aka Linux PAM) before 1.6.0 allows attackers to cause a denial of service (blocked

Mitigation: No fix available

CVE ID: CVE-2023-31484

Description: CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over H

Mitigation: No fix available

CVE ID: CVE-2011-4116

Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.

Mitigation: No fix available

CVE ID: CVE-2023-31486
Description: HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN
Mitigation: No fix available

CVE ID: CVE-2023-37769
Description: stress-test master commit e4c878 was discovered to contain a FPE vulnerability via the comp
Mitigation: No fix available

CVE ID: CVE-2023-37769
Description: stress-test master commit e4c878 was discovered to contain a FPE vulnerability via the comp
Mitigation: No fix available

CVE ID: CVE-2021-4214
Description: A heap overflow flaw was found in libpngs' pngimage.c program. This flaw allows an attacker
Mitigation: No fix available

CVE ID: CVE-2021-4214
Description: A heap overflow flaw was found in libpngs' pngimage.c program. This flaw allows an attacker
Mitigation: No fix available

CVE ID: CVE-2023-4016
Description: Under some circumstances, this weakness allows a user who has access to run the “ps” utility
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2021-45346
Description: A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciousl
Mitigation: No fix available

CVE ID: CVE-2021-45346
Description: A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciousl
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2024-46901
Description: Insufficient validation of filenames against control characters in Apache Subversion repositorie
Mitigation: No fix available

CVE ID: CVE-2013-4392
Description: systemd, when updating file permissions, allows local users to change the permissions and S
Mitigation: No fix available

CVE ID: CVE-2023-31437
Description: An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, i
Mitigation: No fix available

CVE ID: CVE-2023-31438
Description: An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then r
Mitigation: No fix available

CVE ID: CVE-2023-31439
Description: An issue was discovered in systemd 253. An attacker can modify the contents of past events
Mitigation: No fix available

CVE ID: CVE-2021-35331
Description: In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a craft
Mitigation: No fix available

CVE ID: CVE-2023-52355
Description: An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file t
Mitigation: No fix available

CVE ID: CVE-2023-6277
Description: An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may all
Mitigation: No fix available

CVE ID: CVE-2017-16232
Description: LibTIFF 4.0.8 has multiple memory leak vulnerabilities, which allow attackers to cause a denia
Mitigation: No fix available

CVE ID: CVE-2017-17973
Description: In LibTIFF 4.0.8, there is a heap-based use-after-free in the t2p_writeproc function in tiff2pdf.c
Mitigation: No fix available

CVE ID: CVE-2017-5563
Description: LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in D
Mitigation: No fix available

CVE ID: CVE-2017-9117
Description: In LibTIFF 4.0.6 and possibly other versions, the program processes BMP images without ver
Mitigation: No fix available

CVE ID: CVE-2018-10126
Description: ijg-libjpeg before 9d, as used in tiff2pdf (from LibTIFF) and other products, does not check for
Mitigation: No fix available

CVE ID: CVE-2022-1210
Description: A vulnerability classified as problematic was found in LibTIFF 4.3.0. Affected by this vulnerabi
Mitigation: No fix available

CVE ID: CVE-2023-1916
Description: A flaw was found in tiffcrop, a program distributed by the libtiff package. A specially crafted tiff
Mitigation: No fix available

CVE ID: CVE-2023-3164
Description: A heap-buffer-overflow vulnerability was found in LibTIFF, in extractImageSection() at tools/tif
Mitigation: No fix available

CVE ID: CVE-2023-6228
Description: An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF fil
Mitigation: No fix available

CVE ID: CVE-2023-52355
Description: An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file t
Mitigation: No fix available

CVE ID: CVE-2023-6277
Description: An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may all
Mitigation: No fix available

CVE ID: CVE-2017-16232
Description: LibTIFF 4.0.8 has multiple memory leak vulnerabilities, which allow attackers to cause a denia
Mitigation: No fix available

CVE ID: CVE-2017-17973
Description: In LibTIFF 4.0.8, there is a heap-based use-after-free in the t2p_writeproc function in tiff2pdf.c
Mitigation: No fix available

CVE ID: CVE-2017-5563
Description: LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in D
Mitigation: No fix available

CVE ID: CVE-2017-9117
Description: In LibTIFF 4.0.6 and possibly other versions, the program processes BMP images without ver
Mitigation: No fix available

CVE ID: CVE-2018-10126
Description: ijg-libjpeg before 9d, as used in tiff2pdf (from LibTIFF) and other products, does not check for
Mitigation: No fix available

CVE ID: CVE-2022-1210
Description: A vulnerability classified as problematic was found in LibTIFF 4.3.0. Affected by this vulnerabi
Mitigation: No fix available

CVE ID: CVE-2023-1916
Description: A flaw was found in tiffcrop, a program distributed by the libtiff package. A specially crafted tiff
Mitigation: No fix available

CVE ID: CVE-2023-3164
Description: A heap-buffer-overflow vulnerability was found in LibTIFF, in extractImageSection() at tools/tif
Mitigation: No fix available

CVE ID: CVE-2023-6228
Description: An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF fil
Mitigation: No fix available

CVE ID: CVE-2023-52355
Description: An out-of-memory flaw was found in libtiff that could be triggered by passing a crafted tiff file t
Mitigation: No fix available

CVE ID: CVE-2023-6277
Description: An out-of-memory flaw was found in libtiff. Passing a crafted tiff file to TIFFOpen() API may all
Mitigation: No fix available

CVE ID: CVE-2017-16232
Description: LibTIFF 4.0.8 has multiple memory leak vulnerabilities, which allow attackers to cause a denia
Mitigation: No fix available

CVE ID: CVE-2017-17973
Description: In LibTIFF 4.0.8, there is a heap-based use-after-free in the t2p_writeproc function in tiff2pdf.c
Mitigation: No fix available

CVE ID: CVE-2017-5563
Description: LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in D
Mitigation: No fix available

CVE ID: CVE-2017-9117
Description: In LibTIFF 4.0.6 and possibly other versions, the program processes BMP images without ver
Mitigation: No fix available

CVE ID: CVE-2018-10126
Description: ijg-libjpeg before 9d, as used in tiff2pdf (from LibTIFF) and other products, does not check for
Mitigation: No fix available

CVE ID: CVE-2022-1210
Description: A vulnerability classified as problematic was found in LibTIFF 4.3.0. Affected by this vulnerabi
Mitigation: No fix available

CVE ID: CVE-2023-1916
Description: A flaw was found in tiffcrop, a program distributed by the libtiff package. A specially crafted tiff
Mitigation: No fix available

CVE ID: CVE-2023-3164
Description: A heap-buffer-overflow vulnerability was found in LibTIFF, in extractImageSection() at tools/tif
Mitigation: No fix available

CVE ID: CVE-2023-6228
Description: An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF fil
Mitigation: No fix available

CVE ID: CVE-2023-50495
Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2022-27943
Description: libiberty/rust-demangle.c in GNU GCC 11.2 allows stack consumption in demangle_const, as
Mitigation: No fix available

CVE ID: CVE-2023-4039
Description: ■■**DISPUTED**A failure in the -fstack-protector feature in GCC-based toolchains ■that targ
Mitigation: No fix available

CVE ID: CVE-2013-4392
Description: systemd, when updating file permissions, allows local users to change the permissions and S
Mitigation: No fix available

CVE ID: CVE-2023-31437
Description: An issue was discovered in systemd 253. An attacker can modify a sealed log file such that, i
Mitigation: No fix available

CVE ID: CVE-2023-31438
Description: An issue was discovered in systemd 253. An attacker can truncate a sealed log file and then r
Mitigation: No fix available

CVE ID: CVE-2023-31439
Description: An issue was discovered in systemd 253. An attacker can modify the contents of past events
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2007-3476
Description: Array index error in gd_gif_in.c in the GD Graphics Library (libgd) before 2.0.35 allows user-as
Mitigation: No fix available

CVE ID: CVE-2007-3477
Description: The (a) imagearc and (b) imagefilledarc functions in GD Graphics Library (libgd) before 2.0.35
Mitigation: No fix available

CVE ID: CVE-2007-3996
Description: Multiple integer overflows in libgd in PHP before 5.2.4 allow remote attackers to cause a denia
Mitigation: No fix available

CVE ID: CVE-2009-3546
Description: The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Grap
Mitigation: No fix available

CVE ID: TEMP-0601525-BEBB65
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2007-3476
Description: Array index error in gd_gif_in.c in the GD Graphics Library (libgd) before 2.0.35 allows user-as
Mitigation: No fix available

CVE ID: CVE-2007-3477
Description: The (a) imagearc and (b) imagefilledarc functions in GD Graphics Library (libgd) before 2.0.35
Mitigation: No fix available

CVE ID: CVE-2007-3996
Description: Multiple integer overflows in libgd in PHP before 5.2.4 allow remote attackers to cause a denia
Mitigation: No fix available

CVE ID: CVE-2009-3546
Description: The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Grap
Mitigation: No fix available

CVE ID: TEMP-0601525-BEBB65
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2007-3476
Description: Array index error in gd_gif_in.c in the GD Graphics Library (libgd) before 2.0.35 allows user-as
Mitigation: No fix available

CVE ID: CVE-2007-3477
Description: The (a) imagearc and (b) imagefilledarc functions in GD Graphics Library (libgd) before 2.0.35
Mitigation: No fix available

CVE ID: CVE-2007-3996
Description: Multiple integer overflows in libgd in PHP before 5.2.4 allow remote attackers to cause a denia
Mitigation: No fix available

CVE ID: CVE-2009-3546
Description: The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Grap
Mitigation: No fix available

CVE ID: TEMP-0601525-BEBB65
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2024-25062
Description: An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the X
Mitigation: No fix available

CVE ID: CVE-2023-39615
Description: Xmlsoft Libxml2 v2.11.0 was discovered to contain an out-of-bounds read via the xmlSAX2Sta
Mitigation: No fix available

CVE ID: CVE-2023-45322
Description: libxml2 through 2.11.5 has a use-after-free that can only occur after a certain memory allocati
Mitigation: No fix available

CVE ID: CVE-2024-34459
Description: An issue was discovered in xmllint (from libxml2) before 2.11.8 and 2.12.x before 2.12.7. Form
Mitigation: No fix available

CVE ID: CVE-2024-25062
Description: An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.12.5. When using the XI
Mitigation: No fix available

CVE ID: CVE-2023-39615
Description: Xmlsoft Libxml2 v2.11.0 was discovered to contain an out-of-bounds read via the xmlSAX2Sta
Mitigation: No fix available

CVE ID: CVE-2023-45322
Description: libxml2 through 2.11.5 has a use-after-free that can only occur after a certain memory allocati
Mitigation: No fix available

CVE ID: CVE-2024-34459
Description: An issue was discovered in xmllint (from libxml2) before 2.11.8 and 2.12.x before 2.12.7. Form
Mitigation: No fix available

CVE ID: CVE-2015-9019
Description: In libxslt 1.1.29 and earlier, the EXSLT math.random function was not initialized with a random
Mitigation: No fix available

CVE ID: CVE-2015-9019
Description: In libxslt 1.1.29 and earlier, the EXSLT math.random function was not initialized with a random
Mitigation: No fix available

CVE ID: CVE-2013-7445
Description: The Direct Rendering Manager (DRM) subsystem in the Linux kernel through 4.x mishandles
Mitigation: No fix available

CVE ID: CVE-2019-19449
Description: In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can lead to slab-out-of-bo
Mitigation: No fix available

CVE ID: CVE-2019-19814
Description: In the Linux kernel 5.0.21, mounting a crafted f2fs filesystem image can cause __remove_dirty
Mitigation: No fix available

CVE ID: CVE-2021-3847
Description: An unauthorized access to the execution of the setuid file with capabilities flaw in the Linux ke
Mitigation: No fix available

CVE ID: CVE-2021-3864
Description: A flaw was found in the way the dumpable flag setting was handled when certain SUID binarie
Mitigation: No fix available

CVE ID: CVE-2023-52452
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Fix accesses to unini
Mitigation: No fix available

CVE ID: CVE-2023-52590
Description: In the Linux kernel, the following vulnerability has been resolved:■■ocfs2: Avoid touching ren
Mitigation: No fix available

CVE ID: CVE-2023-52751
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: fix use-after-f
Mitigation: No fix available

CVE ID: CVE-2024-21803
Description: Use After Free vulnerability in Linux Linux kernel kernel on Linux, x86, ARM (bluetooth modul
Mitigation: No fix available

CVE ID: CVE-2024-25742
Description: In the Linux kernel before 6.9, an untrusted hypervisor can inject virtual interrupt 29 (#VC) at a
Mitigation: No fix available

CVE ID: CVE-2024-25743
Description: In the Linux kernel through 6.9, an untrusted hypervisor can inject virtual interrupts 0 and 14 a
Mitigation: No fix available

CVE ID: CVE-2024-26669
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/sched: flower: Fix cha
Mitigation: No fix available

CVE ID: CVE-2024-26739
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/sched: act_mirred: do
Mitigation: No fix available

CVE ID: CVE-2024-26913
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix dcn
Mitigation: No fix available

CVE ID: CVE-2024-26930
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: qla2xxx: Fix double
Mitigation: No fix available

CVE ID: CVE-2024-26944
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: zoned: fix use-after-
Mitigation: No fix available

CVE ID: CVE-2024-27042
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: Fix potentia
Mitigation: No fix available

CVE ID: CVE-2024-35866
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: fix potential U
Mitigation: No fix available

CVE ID: CVE-2024-35887
Description: In the Linux kernel, the following vulnerability has been resolved:■■ax25: fix use-after-free bu
Mitigation: No fix available

CVE ID: CVE-2024-35929
Description: In the Linux kernel, the following vulnerability has been resolved:■■rcu/nocb: Fix WARN_ON_
Mitigation: No fix available

CVE ID: CVE-2024-36013
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: L2CAP: Fix sla
Mitigation: No fix available

CVE ID: CVE-2024-36899
Description: In the Linux kernel, the following vulnerability has been resolved:■■gpiolib: cdev: Fix use afte
Mitigation: No fix available

CVE ID: CVE-2024-38570
Description: In the Linux kernel, the following vulnerability has been resolved:■■gfs2: Fix potential glock u
Mitigation: No fix available

CVE ID: CVE-2024-38630
Description: In the Linux kernel, the following vulnerability has been resolved:■■watchdog: cpu5wdt.c: Fix
Mitigation: No fix available

CVE ID: CVE-2024-39479
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/i915/hwmon: Get rid
Mitigation: No fix available

CVE ID: CVE-2024-39508
Description: In the Linux kernel, the following vulnerability has been resolved:■■io_uring/io-wq: Use set_b
Mitigation: No fix available

CVE ID: CVE-2024-41013
Description: In the Linux kernel, the following vulnerability has been resolved:■■xfs: don't walk off the end
Mitigation: No fix available

CVE ID: CVE-2024-41061
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix arra
Mitigation: No fix available

CVE ID: CVE-2024-42162
Description: In the Linux kernel, the following vulnerability has been resolved:■■gve: Account for stopped
Mitigation: No fix available

CVE ID: CVE-2024-44941
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to cover read exte
Mitigation: No fix available

CVE ID: CVE-2024-44942
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to do sanity check
Mitigation: No fix available

CVE ID: CVE-2024-44951
Description: In the Linux kernel, the following vulnerability has been resolved:■■serial: sc16is7xx: fix TX fi
Mitigation: No fix available

CVE ID: CVE-2024-46774
Description: In the Linux kernel, the following vulnerability has been resolved:■■powerpc/rtas: Prevent Sp
Mitigation: No fix available

CVE ID: CVE-2024-46786
Description: In the Linux kernel, the following vulnerability has been resolved:■■fscache: delete fscache_c
Mitigation: No fix available

CVE ID: CVE-2024-46811
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix inde
Mitigation: No fix available

CVE ID: CVE-2024-46813
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check l
Mitigation: No fix available

CVE ID: CVE-2024-46820
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu/vcn: remove
Mitigation: No fix available

CVE ID: CVE-2024-46833
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: hns3: void array out
Mitigation: No fix available

CVE ID: CVE-2024-47691
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to avoid use-after
Mitigation: No fix available

CVE ID: CVE-2024-49928
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: rtw89: avoid reading
Mitigation: No fix available

CVE ID: CVE-2024-49989
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: fix doub
Mitigation: No fix available

CVE ID: CVE-2024-50029
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: hci_conn: Fix U
Mitigation: No fix available

CVE ID: CVE-2024-50047
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: fix UAF in asy
Mitigation: No fix available

CVE ID: CVE-2024-50061
Description: In the Linux kernel, the following vulnerability has been resolved:■■i3c: master: cdns: Fix use
Mitigation: No fix available

CVE ID: CVE-2024-50063
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Prevent tail call betw
Mitigation: No fix available

CVE ID: CVE-2024-50112
Description: In the Linux kernel, the following vulnerability has been resolved:■■x86/lam: Disable ADDRE
Mitigation: No fix available

CVE ID: CVE-2024-50164
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Fix overloading of ME
Mitigation: No fix available

CVE ID: CVE-2024-50217
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: fix use-after-free of
Mitigation: No fix available

CVE ID: CVE-2024-50226
Description: In the Linux kernel, the following vulnerability has been resolved:■■cxl/port: Fix use-after-free
Mitigation: No fix available

CVE ID: CVE-2024-50246
Description: In the Linux kernel, the following vulnerability has been resolved:■■fs/ntfs3: Add rough attr al
Mitigation: No fix available

CVE ID: CVE-2024-53068
Description: In the Linux kernel, the following vulnerability has been resolved:■■firmware: arm_scmi: Fix s
Mitigation: No fix available

CVE ID: CVE-2024-53108
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Adjust V
Mitigation: No fix available

CVE ID: CVE-2024-53133
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Handle
Mitigation: No fix available

CVE ID: CVE-2024-53179
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: fix use-after-f
Mitigation: No fix available

CVE ID: CVE-2024-53229
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/rxe: Fix the qp flus
Mitigation: No fix available

CVE ID: CVE-2024-56538
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm: zynqmp_kms: Unplu
Mitigation: No fix available

CVE ID: CVE-2024-56582
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: fix use-after-free in
Mitigation: No fix available

CVE ID: CVE-2024-56608
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix out-
Mitigation: No fix available

CVE ID: CVE-2024-56631
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: sg: Fix slab-use-afte
Mitigation: No fix available

CVE ID: CVE-2024-56664
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf, sockmap: Fix race be
Mitigation: No fix available

CVE ID: CVE-2024-56759
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: fix use-after-free wh
Mitigation: No fix available

CVE ID: CVE-2024-56775
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix han
Mitigation: No fix available

CVE ID: CVE-2024-56784
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Adding
Mitigation: No fix available

CVE ID: CVE-2019-15213
Description: An issue was discovered in the Linux kernel before 5.2.3. There is a use-after-free caused by
Mitigation: No fix available

CVE ID: CVE-2019-16089
Description: An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/
Mitigation: No fix available

CVE ID: CVE-2019-20794
Description: An issue was discovered in the Linux kernel 4.18 through 5.6.11 when unprivileged user nam
Mitigation: No fix available

CVE ID: CVE-2020-14304
Description: A memory disclosure flaw was found in the Linux kernel's ethernet drivers, in the way it read d
Mitigation: No fix available

CVE ID: CVE-2020-36694
Description: An issue was discovered in netfilter in the Linux kernel before 5.10. There can be a use-after-
Mitigation: No fix available

CVE ID: CVE-2023-0597
Description: A flaw possibility of memory leak in the Linux kernel cpu_entry_area mapping of X86 CPU dat
Mitigation: No fix available

CVE ID: CVE-2023-21264
Description: In multiple functions of mem_protect.c, there is a possible way to access hypervisor memory d
Mitigation: No fix available

CVE ID: CVE-2023-23005
Description: In the Linux kernel before 6.2, mm/memory-tiers.c misinterprets the alloc_memory_type return
Mitigation: No fix available

CVE ID: CVE-2023-31082
Description: An issue was discovered in drivers/tty/n_gsm.c in the Linux kernel 6.2. There is a sleeping fun
Mitigation: No fix available

CVE ID: CVE-2023-3397
Description: A race condition occurred between the functions lmLogClose and txEnd in JFS, in the Linux K
Mitigation: No fix available

CVE ID: CVE-2023-37454
Description: An issue was discovered in the Linux kernel through 6.4.2. A crafted UDF filesystem image ca
Mitigation: No fix available

CVE ID: CVE-2023-4010
Description: A flaw was found in the USB Host Controller Driver framework in the Linux kernel. The usb_gi
Mitigation: No fix available

CVE ID: CVE-2023-4133
Description: A use-after-free vulnerability was found in the cxgb4 driver in the Linux kernel. The bug occurs
Mitigation: No fix available

CVE ID: CVE-2023-52485
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Wake D
Mitigation: No fix available

CVE ID: CVE-2023-52586
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/msm/dpu: Add mutex
Mitigation: No fix available

CVE ID: CVE-2023-52591
Description: In the Linux kernel, the following vulnerability has been resolved:■■reiserfs: Avoid touching re
Mitigation: No fix available

CVE ID: CVE-2023-52596
Description: In the Linux kernel, the following vulnerability has been resolved:■■sysctl: Fix out of bounds a
Mitigation: No fix available

CVE ID: CVE-2023-52624
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Wake D
Mitigation: No fix available

CVE ID: CVE-2023-52625
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Refacto
Mitigation: No fix available

CVE ID: CVE-2023-52629
Description: In the Linux kernel, the following vulnerability has been resolved:■■sh: push-switch: Reorder
Mitigation: No fix available

CVE ID: CVE-2023-52648
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/vmwgfx: Unmap the
Mitigation: No fix available

CVE ID: CVE-2023-52653
Description: In the Linux kernel, the following vulnerability has been resolved:■■SUNRPC: fix a memleak
Mitigation: No fix available

CVE ID: CVE-2023-52658
Description: In the Linux kernel, the following vulnerability has been resolved:■■Revert "net/mlx5: Block e
Mitigation: No fix available

CVE ID: CVE-2023-52671
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix han
Mitigation: No fix available

CVE ID: CVE-2023-52673
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix a de
Mitigation: No fix available

CVE ID: CVE-2023-52676
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Guard stack limits ag
Mitigation: No fix available

CVE ID: CVE-2023-52761
Description: In the Linux kernel, the following vulnerability has been resolved:■■riscv: VMAP_STACK ove
Mitigation: No fix available

CVE ID: CVE-2023-52770
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: split initial and dynar
Mitigation: No fix available

CVE ID: CVE-2023-52771
Description: In the Linux kernel, the following vulnerability has been resolved:■■cxl/port: Fix delete_endpo
Mitigation: No fix available

CVE ID: CVE-2023-52797
Description: In the Linux kernel, the following vulnerability has been resolved:■■drivers: perf: Check find_
Mitigation: No fix available

CVE ID: CVE-2023-52857
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/mediatek: Fix coverit
Mitigation: No fix available

CVE ID: CVE-2023-52888
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: mediatek: vcodec:
Mitigation: No fix available

CVE ID: CVE-2023-52920
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: support non-r10 regis
Mitigation: No fix available

CVE ID: CVE-2023-6039
Description: A use-after-free flaw was found in lan78xx_disconnect in drivers/net/usb/lan78xx.c in the netw
Mitigation: No fix available

CVE ID: CVE-2023-6240
Description: A Marvin vulnerability side-channel leakage was found in the RSA decryption operation in the
Mitigation: No fix available

CVE ID: CVE-2024-2193
Description: A Speculative Race Condition (SRC) vulnerability that impacts modern CPU architectures sup
Mitigation: No fix available

CVE ID: CVE-2024-24855
Description: A race condition was found in the Linux kernel's scsi device driver in lpfc_unregister_fcf_resca
Mitigation: No fix available

CVE ID: CVE-2024-24864
Description: A race condition was found in the Linux kernel's media/dvb-core in dvbdmx_write() function. T
Mitigation: No fix available

CVE ID: CVE-2024-25740
Description: A memory leak flaw was found in the UBI driver in drivers/mtd/ubi/attach.c in the Linux kernel
Mitigation: No fix available

CVE ID: CVE-2024-26596
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: dsa: fix netdev_priv()
Mitigation: No fix available

CVE ID: CVE-2024-26618
Description: In the Linux kernel, the following vulnerability has been resolved:■■arm64/sme: Always exit s
Mitigation: No fix available

CVE ID: CVE-2024-26647
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix late
Mitigation: No fix available

CVE ID: CVE-2024-26648
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix vari
Mitigation: No fix available

CVE ID: CVE-2024-26656
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: fix use-after
Mitigation: No fix available

CVE ID: CVE-2024-26661
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add NU
Mitigation: No fix available

CVE ID: CVE-2024-26662
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix 'par
Mitigation: No fix available

CVE ID: CVE-2024-26670
Description: In the Linux kernel, the following vulnerability has been resolved:■■arm64: entry: fix ARM64_
Mitigation: No fix available

CVE ID: CVE-2024-26672
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: Fix variable
Mitigation: No fix available

CVE ID: CVE-2024-26677
Description: In the Linux kernel, the following vulnerability has been resolved:■■rxrpc: Fix delayed ACKs t
Mitigation: No fix available

CVE ID: CVE-2024-26691
Description: In the Linux kernel, the following vulnerability has been resolved:■■KVM: arm64: Fix circular
Mitigation: No fix available

CVE ID: CVE-2024-26719
Description: In the Linux kernel, the following vulnerability has been resolved:■■nouveau: offload fence ue
Mitigation: No fix available

CVE ID: CVE-2024-26740
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/sched: act_mirred: us
Mitigation: No fix available

CVE ID: CVE-2024-26756
Description: In the Linux kernel, the following vulnerability has been resolved:■■md: Don't register sync_tl
Mitigation: No fix available

CVE ID: CVE-2024-26757
Description: In the Linux kernel, the following vulnerability has been resolved:■■md: Don't ignore read-onl
Mitigation: No fix available

CVE ID: CVE-2024-26758
Description: In the Linux kernel, the following vulnerability has been resolved:■■md: Don't ignore suspend
Mitigation: No fix available

CVE ID: CVE-2024-26767
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: fixed int
Mitigation: No fix available

CVE ID: CVE-2024-26768
Description: In the Linux kernel, the following vulnerability has been resolved:■■LoongArch: Change acpi_
Mitigation: No fix available

CVE ID: CVE-2024-26783
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/vmscan: fix a bug cal
Mitigation: No fix available

CVE ID: CVE-2024-26799
Description: In the Linux kernel, the following vulnerability has been resolved:■■ASoC: qcom: Fix uninitial
Mitigation: No fix available

CVE ID: CVE-2024-26807
Description: In the Linux kernel, the following vulnerability has been resolved:■■Both cadence-quadspi ->
Mitigation: No fix available

CVE ID: CVE-2024-26822
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: set correct id,
Mitigation: No fix available

CVE ID: CVE-2024-26836
Description: In the Linux kernel, the following vulnerability has been resolved:■■platform/x86: think-lmi: Fi
Mitigation: No fix available

CVE ID: CVE-2024-26841
Description: In the Linux kernel, the following vulnerability has been resolved:■■LoongArch: Update cpu_s
Mitigation: No fix available

CVE ID: CVE-2024-26842
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: ufs: core: Fix shift iss
Mitigation: No fix available

CVE ID: CVE-2024-26866
Description: In the Linux kernel, the following vulnerability has been resolved:■■spi: lpspi: Avoid potential
Mitigation: No fix available

CVE ID: CVE-2024-26869
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to truncate meta i
Mitigation: No fix available

CVE ID: CVE-2024-26876
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/bridge: adv7511: fix c
Mitigation: No fix available

CVE ID: CVE-2024-26902
Description: In the Linux kernel, the following vulnerability has been resolved:■■perf: RISCV: Fix panic on
Mitigation: No fix available

CVE ID: CVE-2024-26914
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: fix incor
Mitigation: No fix available

CVE ID: CVE-2024-26947
Description: In the Linux kernel, the following vulnerability has been resolved:■■ARM: 9359/1: flush: chec
Mitigation: No fix available

CVE ID: CVE-2024-26948
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add a c
Mitigation: No fix available

CVE ID: CVE-2024-26953
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: esp: fix bad handling
Mitigation: No fix available

CVE ID: CVE-2024-26962
Description: In the Linux kernel, the following vulnerability has been resolved:■■dm-raid456, md/raid456:
Mitigation: No fix available

CVE ID: CVE-2024-26982
Description: In the Linux kernel, the following vulnerability has been resolved:■■Squashfs: check the inod
Mitigation: No fix available

CVE ID: CVE-2024-27005
Description: In the Linux kernel, the following vulnerability has been resolved:■■interconnect: Don't acces
Mitigation: No fix available

CVE ID: CVE-2024-27010
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/sched: Fix mirred dea
Mitigation: No fix available

CVE ID: CVE-2024-27011
Description: In the Linux kernel, the following vulnerability has been resolved:■■netfilter: nf_tables: fix me
Mitigation: No fix available

CVE ID: CVE-2024-27012
Description: In the Linux kernel, the following vulnerability has been resolved:■■netfilter: nf_tables: restore
Mitigation: No fix available

CVE ID: CVE-2024-27041
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: fix NUL
Mitigation: No fix available

CVE ID: CVE-2024-27056
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: iwlwifi: mvm: ensure
Mitigation: No fix available

CVE ID: CVE-2024-27057
Description: In the Linux kernel, the following vulnerability has been resolved:■■ASoC: SOF: ipc4-pcm: W
Mitigation: No fix available

CVE ID: CVE-2024-27062
Description: In the Linux kernel, the following vulnerability has been resolved:■■nouveau: lock the client o
Mitigation: No fix available

CVE ID: CVE-2024-27079
Description: In the Linux kernel, the following vulnerability has been resolved:■■iommu/vt-d: Fix NULL do
Mitigation: No fix available

CVE ID: CVE-2024-27408
Description: In the Linux kernel, the following vulnerability has been resolved:■■dmaengine: dw-edma: eD
Mitigation: No fix available

CVE ID: CVE-2024-35784
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: fix deadlock with fie
Mitigation: No fix available

CVE ID: CVE-2024-35790
Description: In the Linux kernel, the following vulnerability has been resolved:■■usb: typec: altmodes/disp
Mitigation: No fix available

CVE ID: CVE-2024-35794
Description: In the Linux kernel, the following vulnerability has been resolved:■■dm-raid: really frozen syn
Mitigation: No fix available

CVE ID: CVE-2024-35799
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Prevent
Mitigation: No fix available

CVE ID: CVE-2024-35808
Description: In the Linux kernel, the following vulnerability has been resolved:■■md/dm-raid: don't call md
Mitigation: No fix available

CVE ID: CVE-2024-35843
Description: In the Linux kernel, the following vulnerability has been resolved:■■iommu/vt-d: Use device rl
Mitigation: No fix available

CVE ID: CVE-2024-35860
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: support deferring bpf
Mitigation: No fix available

CVE ID: CVE-2024-35869
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: guarantee ref
Mitigation: No fix available

CVE ID: CVE-2024-35878
Description: In the Linux kernel, the following vulnerability has been resolved:■■of: module: prevent NULL
Mitigation: No fix available

CVE ID: CVE-2024-35904
Description: In the Linux kernel, the following vulnerability has been resolved:■■selinux: avoid dereferenc
Mitigation: No fix available

CVE ID: CVE-2024-35924
Description: In the Linux kernel, the following vulnerability has been resolved:■■usb: typec: ucsi: Limit rea
Mitigation: No fix available

CVE ID: CVE-2024-35931
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: Skip do PC
Mitigation: No fix available

CVE ID: CVE-2024-35942
Description: In the Linux kernel, the following vulnerability has been resolved:■■pmdomain: imx8mp-blk-c
Mitigation: No fix available

CVE ID: CVE-2024-35945
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: phy: phy_device: Pre
Mitigation: No fix available

CVE ID: CVE-2024-35946
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: rtw89: fix null pointer
Mitigation: No fix available

CVE ID: CVE-2024-35949
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: make sure that WR
Mitigation: No fix available

CVE ID: CVE-2024-35951
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/panfrost: Fix the erro
Mitigation: No fix available

CVE ID: CVE-2024-35961
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/mlx5: Register devlink
Mitigation: No fix available

CVE ID: CVE-2024-35974
Description: In the Linux kernel, the following vulnerability has been resolved:■■block: fix q->blkg_list corr
Mitigation: No fix available

CVE ID: CVE-2024-36022
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: Init zone de
Mitigation: No fix available

CVE ID: CVE-2024-36024
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Disable
Mitigation: No fix available

CVE ID: CVE-2024-36476
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/rtrs: Ensure 'ib_sg
Mitigation: No fix available

CVE ID: CVE-2024-36881
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/userfaultfd: reset ptes
Mitigation: No fix available

CVE ID: CVE-2024-36903
Description: In the Linux kernel, the following vulnerability has been resolved:■■ipv6: Fix potential uninit-v
Mitigation: No fix available

CVE ID: CVE-2024-36907
Description: In the Linux kernel, the following vulnerability has been resolved:■■SUNRPC: add a missing
Mitigation: No fix available

CVE ID: CVE-2024-36908
Description: In the Linux kernel, the following vulnerability has been resolved:■■blk-iocost: do not WARN
Mitigation: No fix available

CVE ID: CVE-2024-36911
Description: In the Linux kernel, the following vulnerability has been resolved:■■hv_netvsc: Don't free dec
Mitigation: No fix available

CVE ID: CVE-2024-36913
Description: In the Linux kernel, the following vulnerability has been resolved:■■Drivers: hv: vmbus: Leak
Mitigation: No fix available

CVE ID: CVE-2024-36921
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: iwlwifi: mvm: guard a
Mitigation: No fix available

CVE ID: CVE-2024-36922
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: iwlwifi: read txq->rea
Mitigation: No fix available

CVE ID: CVE-2024-36927
Description: In the Linux kernel, the following vulnerability has been resolved:■■ipv4: Fix uninit-value acce
Mitigation: No fix available

CVE ID: CVE-2024-36949
Description: In the Linux kernel, the following vulnerability has been resolved:■■amd/amdkfd: sync all dev
Mitigation: No fix available

CVE ID: CVE-2024-36951
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdkfd: range check
Mitigation: No fix available

CVE ID: CVE-2024-36968
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: L2CAP: Fix div
Mitigation: No fix available

CVE ID: CVE-2024-38541
Description: In the Linux kernel, the following vulnerability has been resolved:■■of: module: add buffer ov
Mitigation: No fix available

CVE ID: CVE-2024-38557
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/mlx5: Reload only IB
Mitigation: No fix available

CVE ID: CVE-2024-38564
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Add BPF_PROG_TY
Mitigation: No fix available

CVE ID: CVE-2024-38594
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: stmmac: move the E
Mitigation: No fix available

CVE ID: CVE-2024-38608
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/mlx5e: Fix netif state
Mitigation: No fix available

CVE ID: CVE-2024-38611
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: i2c: et8ek8: Don't
Mitigation: No fix available

CVE ID: CVE-2024-38620
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: HCI: Remove
Mitigation: No fix available

CVE ID: CVE-2024-38622
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/msm/dpu: Add callba
Mitigation: No fix available

CVE ID: CVE-2024-38625
Description: In the Linux kernel, the following vulnerability has been resolved:■■fs/ntfs3: Check 'folio' poin
Mitigation: No fix available

CVE ID: CVE-2024-39282
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: wwan: t7xx: Fix FSM
Mitigation: No fix available

CVE ID: CVE-2024-39293
Description: In the Linux kernel, the following vulnerability has been resolved:■■Revert "xsk: Support redi
Mitigation: No fix available

CVE ID: CVE-2024-40945
Description: In the Linux kernel, the following vulnerability has been resolved:■■iommu: Return right value
Mitigation: No fix available

CVE ID: CVE-2024-40965
Description: In the Linux kernel, the following vulnerability has been resolved:■■i2c: lpi2c: Avoid calling cl
Mitigation: No fix available

CVE ID: CVE-2024-40969
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: don't set RO when s
Mitigation: No fix available

CVE ID: CVE-2024-40973
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: mtk-vcodec: poter
Mitigation: No fix available

CVE ID: CVE-2024-40975
Description: In the Linux kernel, the following vulnerability has been resolved:■■platform/x86: x86-androi
Mitigation: No fix available

CVE ID: CVE-2024-40982
Description: In the Linux kernel, the following vulnerability has been resolved:■■ssb: Fix potential NULL p
Mitigation: No fix available

CVE ID: CVE-2024-40997
Description: In the Linux kernel, the following vulnerability has been resolved:■■cpufreq: amd-pstate: fix n
Mitigation: No fix available

CVE ID: CVE-2024-40998
Description: In the Linux kernel, the following vulnerability has been resolved:■■ext4: fix uninitialized ratel
Mitigation: No fix available

CVE ID: CVE-2024-40999
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: ena: Add validation fo
Mitigation: No fix available

CVE ID: CVE-2024-41008
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: change vm-
Mitigation: No fix available

CVE ID: CVE-2024-41023
Description: In the Linux kernel, the following vulnerability has been resolved:■■sched/deadline: Fix task_
Mitigation: No fix available

CVE ID: CVE-2024-41031
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/filemap: skip to creat
Mitigation: No fix available

CVE ID: CVE-2024-41045
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Defer work in bpf_tim
Mitigation: No fix available

CVE ID: CVE-2024-41067
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: scrub: handle RST l
Mitigation: No fix available

CVE ID: CVE-2024-41082
Description: In the Linux kernel, the following vulnerability has been resolved:■■nvme-fabrics: use reserve
Mitigation: No fix available

CVE ID: CVE-2024-41935
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to shrink read ext
Mitigation: No fix available

CVE ID: CVE-2024-42064
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Skip pip
Mitigation: No fix available

CVE ID: CVE-2024-42067
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Take return from set_
Mitigation: No fix available

CVE ID: CVE-2024-42079
Description: In the Linux kernel, the following vulnerability has been resolved:■■gfs2: Fix NULL pointer de
Mitigation: No fix available

CVE ID: CVE-2024-42107
Description: In the Linux kernel, the following vulnerability has been resolved:■■ice: Don't process extts if
Mitigation: No fix available

CVE ID: CVE-2024-42117
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: ASSER
Mitigation: No fix available

CVE ID: CVE-2024-42118
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Do not
Mitigation: No fix available

CVE ID: CVE-2024-42122
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add NU
Mitigation: No fix available

CVE ID: CVE-2024-42123
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: fix double fr
Mitigation: No fix available

CVE ID: CVE-2024-42125
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: rtw89: fw: scan offloa
Mitigation: No fix available

CVE ID: CVE-2024-42128
Description: In the Linux kernel, the following vulnerability has been resolved:■■leds: an30259a: Use dev
Mitigation: No fix available

CVE ID: CVE-2024-42129
Description: In the Linux kernel, the following vulnerability has been resolved:■■leds: mlxreg: Use devm_
Mitigation: No fix available

CVE ID: CVE-2024-42134
Description: In the Linux kernel, the following vulnerability has been resolved:■■virtio-pci: Check if is_avq
Mitigation: No fix available

CVE ID: CVE-2024-42135
Description: In the Linux kernel, the following vulnerability has been resolved:■■vhost_task: Handle SIGK
Mitigation: No fix available

CVE ID: CVE-2024-42139
Description: In the Linux kernel, the following vulnerability has been resolved:■■ice: Fix improper extts ha
Mitigation: No fix available

CVE ID: CVE-2024-42144
Description: In the Linux kernel, the following vulnerability has been resolved:■■thermal/drivers/mediatek/
Mitigation: No fix available

CVE ID: CVE-2024-42151
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: mark bpf_dummy_st
Mitigation: No fix available

CVE ID: CVE-2024-42156
Description: In the Linux kernel, the following vulnerability has been resolved:■■s390/pkey: Wipe copies c
Mitigation: No fix available

CVE ID: CVE-2024-42158
Description: In the Linux kernel, the following vulnerability has been resolved:■■s390/pkey: Use kfree_se
Mitigation: No fix available

CVE ID: CVE-2024-42227
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix ove
Mitigation: No fix available

CVE ID: CVE-2024-42239
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Fail bpf_timer_cance
Mitigation: No fix available

CVE ID: CVE-2024-42241
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/shmem: disable PMD
Mitigation: No fix available

CVE ID: CVE-2024-42243
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/filemap: make MAX_
Mitigation: No fix available

CVE ID: CVE-2024-42279
Description: In the Linux kernel, the following vulnerability has been resolved:■■spi: microchip-core: ensu
Mitigation: No fix available

CVE ID: CVE-2024-42317
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/huge_memory: avoid
Mitigation: No fix available

CVE ID: CVE-2024-43819
Description: In the Linux kernel, the following vulnerability has been resolved:■■kvm: s390: Reject memor
Mitigation: No fix available

CVE ID: CVE-2024-43824
Description: In the Linux kernel, the following vulnerability has been resolved:■■PCI: endpoint: pci-epf-tes
Mitigation: No fix available

CVE ID: CVE-2024-43831
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: mediatek: vcodec
Mitigation: No fix available

CVE ID: CVE-2024-43840
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf, arm64: Fix trampolin
Mitigation: No fix available

CVE ID: CVE-2024-43850
Description: In the Linux kernel, the following vulnerability has been resolved:■■soc: qcom: icc-bwmon: Fi
Mitigation: No fix available

CVE ID: CVE-2024-43872
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/hns: Fix soft locku
Mitigation: No fix available

CVE ID: CVE-2024-43886
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add nul
Mitigation: No fix available

CVE ID: CVE-2024-43899
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix null
Mitigation: No fix available

CVE ID: CVE-2024-43901
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix NUL
Mitigation: No fix available

CVE ID: CVE-2024-43906
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/admgpu: fix derefere
Mitigation: No fix available

CVE ID: CVE-2024-43913
Description: In the Linux kernel, the following vulnerability has been resolved:■■nvme: apple: fix device re
Mitigation: No fix available

CVE ID: CVE-2024-44955
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Don't re
Mitigation: No fix available

CVE ID: CVE-2024-44957
Description: In the Linux kernel, the following vulnerability has been resolved:■■xen: privcmd: Switch from
Mitigation: No fix available

CVE ID: CVE-2024-44961
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: Forward so
Mitigation: No fix available

CVE ID: CVE-2024-44963
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: do not BUG_ON() w
Mitigation: No fix available

CVE ID: CVE-2024-44972
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: do not clear page di
Mitigation: No fix available

CVE ID: CVE-2024-45015
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/msm/dpu: move dpu_
Mitigation: No fix available

CVE ID: CVE-2024-46678
Description: In the Linux kernel, the following vulnerability has been resolved:■■bonding: change ipsec_lo
Mitigation: No fix available

CVE ID: CVE-2024-46681
Description: In the Linux kernel, the following vulnerability has been resolved:■■pktgen: use cpus_read_lo
Mitigation: No fix available

CVE ID: CVE-2024-46698
Description: In the Linux kernel, the following vulnerability has been resolved:■■video/aperture: optionally
Mitigation: No fix available

CVE ID: CVE-2024-46727
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add otg
Mitigation: No fix available

CVE ID: CVE-2024-46728
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check i
Mitigation: No fix available

CVE ID: CVE-2024-46729
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Fix incc
Mitigation: No fix available

CVE ID: CVE-2024-46730
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Ensure
Mitigation: No fix available

CVE ID: CVE-2024-46733
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: fix qgroup reserve le
Mitigation: No fix available

CVE ID: CVE-2024-46742
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb/server: fix potential r
Mitigation: No fix available

CVE ID: CVE-2024-46748
Description: In the Linux kernel, the following vulnerability has been resolved:■■cachefiles: Set the max s
Mitigation: No fix available

CVE ID: CVE-2024-46751
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: don't BUG_ON() wh
Mitigation: No fix available

CVE ID: CVE-2024-46753
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: handle errors from b
Mitigation: No fix available

CVE ID: CVE-2024-46754
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Remove tst_run from
Mitigation: No fix available

CVE ID: CVE-2024-46760
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: rtw88: usb: schedule
Mitigation: No fix available

CVE ID: CVE-2024-46762
Description: In the Linux kernel, the following vulnerability has been resolved:■■xen: privcmd: Fix possible
Mitigation: No fix available

CVE ID: CVE-2024-46765
Description: In the Linux kernel, the following vulnerability has been resolved:■■ice: protect XDP configura
Mitigation: No fix available

CVE ID: CVE-2024-46772
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check c
Mitigation: No fix available

CVE ID: CVE-2024-46775
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Validate
Mitigation: No fix available

CVE ID: CVE-2024-46776
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Run DC
Mitigation: No fix available

CVE ID: CVE-2024-46778
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check U
Mitigation: No fix available

CVE ID: CVE-2024-46787
Description: In the Linux kernel, the following vulnerability has been resolved:■■userfaultfd: fix checks for
Mitigation: No fix available

CVE ID: CVE-2024-46803
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdkfd: Check debu
Mitigation: No fix available

CVE ID: CVE-2024-46806
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: Fix the warn
Mitigation: No fix available

CVE ID: CVE-2024-46808
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add mis
Mitigation: No fix available

CVE ID: CVE-2024-46816
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Stop an
Mitigation: No fix available

CVE ID: CVE-2024-46823
Description: In the Linux kernel, the following vulnerability has been resolved:■■kunit/overflow: Fix UB in c
Mitigation: No fix available

CVE ID: CVE-2024-46825
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: iwlwifi: mvm: use IWL
Mitigation: No fix available

CVE ID: CVE-2024-46834
Description: In the Linux kernel, the following vulnerability has been resolved:■■ethtool: fail closed if we ca
Mitigation: No fix available

CVE ID: CVE-2024-46842
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: lpfc: Handle mailbox
Mitigation: No fix available

CVE ID: CVE-2024-46843
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: ufs: core: Remove S
Mitigation: No fix available

CVE ID: CVE-2024-46860
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: mt76: mt7921: fix NU
Mitigation: No fix available

CVE ID: CVE-2024-46861
Description: In the Linux kernel, the following vulnerability has been resolved:■■usbnet: ipheth: do not sto
Mitigation: No fix available

CVE ID: CVE-2024-46870
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Disable
Mitigation: No fix available

CVE ID: CVE-2024-47141
Description: In the Linux kernel, the following vulnerability has been resolved:■■pinmux: Use sequential a
Mitigation: No fix available

CVE ID: CVE-2024-47658
Description: In the Linux kernel, the following vulnerability has been resolved:■■crypto: stm32/cryp - call f
Mitigation: No fix available

CVE ID: CVE-2024-47661
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Avoid o
Mitigation: No fix available

CVE ID: CVE-2024-47662
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Remov
Mitigation: No fix available

CVE ID: CVE-2024-47664
Description: In the Linux kernel, the following vulnerability has been resolved:■■spi: hisi-kunpeng: Add ve
Mitigation: No fix available

CVE ID: CVE-2024-47666
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: pm80xx: Set phy->e
Mitigation: No fix available

CVE ID: CVE-2024-47703
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf, lsm: Add check for B
Mitigation: No fix available

CVE ID: CVE-2024-47704
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check l
Mitigation: No fix available

CVE ID: CVE-2024-47726
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to wait dio comple
Mitigation: No fix available

CVE ID: CVE-2024-47736
Description: In the Linux kernel, the following vulnerability has been resolved:■■erofs: handle overlapped
Mitigation: No fix available

CVE ID: CVE-2024-47752
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: mediatek: vcodec:
Mitigation: No fix available

CVE ID: CVE-2024-47753
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: mediatek: vcodec:
Mitigation: No fix available

CVE ID: CVE-2024-47754
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: mediatek: vcodec:
Mitigation: No fix available

CVE ID: CVE-2024-47794
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Prevent tailcall infinit
Mitigation: No fix available

CVE ID: CVE-2024-47809
Description: In the Linux kernel, the following vulnerability has been resolved:■■dlm: fix possible lkb_reso
Mitigation: No fix available

CVE ID: CVE-2024-48873
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: rtw89: check return v
Mitigation: No fix available

CVE ID: CVE-2024-48875
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: don't take dev_repla
Mitigation: No fix available

CVE ID: CVE-2024-49568
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/smc: check v2_ext_of
Mitigation: No fix available

CVE ID: CVE-2024-49569
Description: In the Linux kernel, the following vulnerability has been resolved:■■nvme-rdma: unquiesce ad
Mitigation: No fix available

CVE ID: CVE-2024-49893
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check s
Mitigation: No fix available

CVE ID: CVE-2024-49901
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/msm/adreno: Assign
Mitigation: No fix available

CVE ID: CVE-2024-49904
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: add list emp
Mitigation: No fix available

CVE ID: CVE-2024-49906
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check r
Mitigation: No fix available

CVE ID: CVE-2024-49908
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add nul
Mitigation: No fix available

CVE ID: CVE-2024-49910
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add NU
Mitigation: No fix available

CVE ID: CVE-2024-49914
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add nul
Mitigation: No fix available

CVE ID: CVE-2024-49916
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add NU
Mitigation: No fix available

CVE ID: CVE-2024-49918
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add nul
Mitigation: No fix available

CVE ID: CVE-2024-49919
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Add nul
Mitigation: No fix available

CVE ID: CVE-2024-49920
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check r
Mitigation: No fix available

CVE ID: CVE-2024-49921
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check r
Mitigation: No fix available

CVE ID: CVE-2024-49922
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Check r
Mitigation: No fix available

CVE ID: CVE-2024-49923
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Pass nc
Mitigation: No fix available

CVE ID: CVE-2024-49926
Description: In the Linux kernel, the following vulnerability has been resolved:■■rcu-tasks: Fix access non
Mitigation: No fix available

CVE ID: CVE-2024-49932
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: don't readahead the
Mitigation: No fix available

CVE ID: CVE-2024-49940
Description: In the Linux kernel, the following vulnerability has been resolved:■■l2tp: prevent possible tun
Mitigation: No fix available

CVE ID: CVE-2024-49945
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/ncsi: Disable the ncsi
Mitigation: No fix available

CVE ID: CVE-2024-49968
Description: In the Linux kernel, the following vulnerability has been resolved:■■ext4: filesystems without
Mitigation: No fix available

CVE ID: CVE-2024-49970
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Implem
Mitigation: No fix available

CVE ID: CVE-2024-49971
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Increas
Mitigation: No fix available

CVE ID: CVE-2024-49972
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Dealloc
Mitigation: No fix available

CVE ID: CVE-2024-49987
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpftool: Fix undefined beh
Mitigation: No fix available

CVE ID: CVE-2024-49988
Description: In the Linux kernel, the following vulnerability has been resolved:■■ksmbd: add refcnt to ksm
Mitigation: No fix available

CVE ID: CVE-2024-49994
Description: In the Linux kernel, the following vulnerability has been resolved:■■block: fix integer overflow
Mitigation: No fix available

CVE ID: CVE-2024-49998
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: dsa: improve shutdo
Mitigation: No fix available

CVE ID: CVE-2024-50004
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: update
Mitigation: No fix available

CVE ID: CVE-2024-50009
Description: In the Linux kernel, the following vulnerability has been resolved:■■cpufreq: amd-pstate: add
Mitigation: No fix available

CVE ID: CVE-2024-50014
Description: In the Linux kernel, the following vulnerability has been resolved:■■ext4: fix access to uninitia
Mitigation: No fix available

CVE ID: CVE-2024-50016
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: Avoid o
Mitigation: No fix available

CVE ID: CVE-2024-50017
Description: In the Linux kernel, the following vulnerability has been resolved:■■x86/mm/ident_map: Use
Mitigation: No fix available

CVE ID: CVE-2024-50028
Description: In the Linux kernel, the following vulnerability has been resolved:■■thermal: core: Reference
Mitigation: No fix available

CVE ID: CVE-2024-50032
Description: In the Linux kernel, the following vulnerability has been resolved:■■rcu/nocb: Fix rcuog wake
Mitigation: No fix available

CVE ID: CVE-2024-50056
Description: In the Linux kernel, the following vulnerability has been resolved:■■usb: gadget: uvc: Fix ERR
Mitigation: No fix available

CVE ID: CVE-2024-50091
Description: In the Linux kernel, the following vulnerability has been resolved:■■dm vdo: don't refer to dec
Mitigation: No fix available

CVE ID: CVE-2024-50111
Description: In the Linux kernel, the following vulnerability has been resolved:■■LoongArch: Enable IRQ if
Mitigation: No fix available

CVE ID: CVE-2024-50135
Description: In the Linux kernel, the following vulnerability has been resolved:■■nvme-pci: fix race conditio
Mitigation: No fix available

CVE ID: CVE-2024-50166
Description: In the Linux kernel, the following vulnerability has been resolved:■■fsl/fman: Fix refcount han
Mitigation: No fix available

CVE ID: CVE-2024-50177
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amd/display: fix a UB
Mitigation: No fix available

CVE ID: CVE-2024-50178
Description: In the Linux kernel, the following vulnerability has been resolved:■■cpufreq: loongson3: Use
Mitigation: No fix available

CVE ID: CVE-2024-50277
Description: In the Linux kernel, the following vulnerability has been resolved:■■dm: fix a crash if blk_alloc
Mitigation: No fix available

CVE ID: CVE-2024-50285
Description: In the Linux kernel, the following vulnerability has been resolved:■■ksmbd: check outstanding
Mitigation: No fix available

CVE ID: CVE-2024-50289
Description: In the Linux kernel, the following vulnerability has been resolved:■■media: av7110: fix a spec
Mitigation: No fix available

CVE ID: CVE-2024-50298
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: enetc: allocate vf_sta
Mitigation: No fix available

CVE ID: CVE-2024-50304
Description: In the Linux kernel, the following vulnerability has been resolved:■■ipv4: ip_tunnel: Fix suspic
Mitigation: No fix available

CVE ID: CVE-2024-53050
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/i915/hdcp: Add enco
Mitigation: No fix available

CVE ID: CVE-2024-53051
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/i915/hdcp: Add enco
Mitigation: No fix available

CVE ID: CVE-2024-53056
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/mediatek: Fix potenti
Mitigation: No fix available

CVE ID: CVE-2024-53079
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/thp: fix deferred split
Mitigation: No fix available

CVE ID: CVE-2024-53085
Description: In the Linux kernel, the following vulnerability has been resolved:■■tpm: Lock TPM chip in tpr
Mitigation: No fix available

CVE ID: CVE-2024-53089
Description: In the Linux kernel, the following vulnerability has been resolved:■■LoongArch: KVM: Mark h
Mitigation: No fix available

CVE ID: CVE-2024-53090
Description: In the Linux kernel, the following vulnerability has been resolved:■■afs: Fix lock recursion■■
Mitigation: No fix available

CVE ID: CVE-2024-53091
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Add sk_is_inet and IS
Mitigation: No fix available

CVE ID: CVE-2024-53094
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/siw: Add sendpag
Mitigation: No fix available

CVE ID: CVE-2024-53095
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: client: Fix use-after-
Mitigation: No fix available

CVE ID: CVE-2024-53114
Description: In the Linux kernel, the following vulnerability has been resolved:■■x86/CPU/AMD: Clear virtu
Mitigation: No fix available

CVE ID: CVE-2024-53124
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: fix data-races around
Mitigation: No fix available

CVE ID: CVE-2024-53128
Description: In the Linux kernel, the following vulnerability has been resolved:■■sched/task_stack: fix obje
Mitigation: No fix available

CVE ID: CVE-2024-53134
Description: In the Linux kernel, the following vulnerability has been resolved:■■pmdomain: imx93-blk-ctrl
Mitigation: No fix available

CVE ID: CVE-2024-53147
Description: In the Linux kernel, the following vulnerability has been resolved:■■exfat: fix out-of-bounds ac
Mitigation: No fix available

CVE ID: CVE-2024-53166
Description: In the Linux kernel, the following vulnerability has been resolved:■■block, bfq: fix bfqq uaf in
Mitigation: No fix available

CVE ID: CVE-2024-53168
Description: In the Linux kernel, the following vulnerability has been resolved:■■sunrpc: fix one UAF issue
Mitigation: No fix available

CVE ID: CVE-2024-53170
Description: In the Linux kernel, the following vulnerability has been resolved:■■block: fix uaf for flush rq w
Mitigation: No fix available

CVE ID: CVE-2024-53176
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: During unmount, en
Mitigation: No fix available

CVE ID: CVE-2024-53177
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: prevent use-after-fre
Mitigation: No fix available

CVE ID: CVE-2024-53178
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: Don't leak cfid when
Mitigation: No fix available

CVE ID: CVE-2024-53187
Description: In the Linux kernel, the following vulnerability has been resolved:■■io_uring: check for overflo
Mitigation: No fix available

CVE ID: CVE-2024-53195
Description: In the Linux kernel, the following vulnerability has been resolved:■■KVM: arm64: Get rid of us
Mitigation: No fix available

CVE ID: CVE-2024-53203
Description: In the Linux kernel, the following vulnerability has been resolved:■■usb: typec: fix potential ar
Mitigation: No fix available

CVE ID: CVE-2024-53209
Description: In the Linux kernel, the following vulnerability has been resolved:■■bnxt_en: Fix receive ring
Mitigation: No fix available

CVE ID: CVE-2024-53216
Description: In the Linux kernel, the following vulnerability has been resolved:■■nfsd: release svc_expkey
Mitigation: No fix available

CVE ID: CVE-2024-53219
Description: In the Linux kernel, the following vulnerability has been resolved:■■virtiofs: use pages instead
Mitigation: No fix available

CVE ID: CVE-2024-53221
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix null-ptr-deref in f2
Mitigation: No fix available

CVE ID: CVE-2024-53224
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/mlx5: Move events
Mitigation: No fix available

CVE ID: CVE-2024-53234
Description: In the Linux kernel, the following vulnerability has been resolved:■■erofs: handle NONHEAD
Mitigation: No fix available

CVE ID: CVE-2024-53685
Description: In the Linux kernel, the following vulnerability has been resolved:■■ceph: give up on paths lo
Mitigation: No fix available

CVE ID: CVE-2024-53687
Description: In the Linux kernel, the following vulnerability has been resolved:■■riscv: Fix IPIs usage in kf
Mitigation: No fix available

CVE ID: CVE-2024-54683
Description: In the Linux kernel, the following vulnerability has been resolved:■■netfilter: IDLETIMER: Fix
Mitigation: No fix available

CVE ID: CVE-2024-56544
Description: In the Linux kernel, the following vulnerability has been resolved:■■udmabuf: change folios a
Mitigation: No fix available

CVE ID: CVE-2024-56549
Description: In the Linux kernel, the following vulnerability has been resolved:■■cachefiles: Fix NULL poin
Mitigation: No fix available

CVE ID: CVE-2024-56551
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdgpu: fix usage sl
Mitigation: No fix available

CVE ID: CVE-2024-56565
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to drop all discard
Mitigation: No fix available

CVE ID: CVE-2024-56566
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/slub: Avoid list corrup
Mitigation: No fix available

CVE ID: CVE-2024-56583
Description: In the Linux kernel, the following vulnerability has been resolved:■■sched/deadline: Fix warni
Mitigation: No fix available

CVE ID: CVE-2024-56588
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: hisi_sas: Create all d
Mitigation: No fix available

CVE ID: CVE-2024-56591
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: hci_conn: Use
Mitigation: No fix available

CVE ID: CVE-2024-56592
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: Call free_htab_elem(
Mitigation: No fix available

CVE ID: CVE-2024-56599
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: ath10k: avoid NULL
Mitigation: No fix available

CVE ID: CVE-2024-56609
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: rtw88: use ieee8021
Mitigation: No fix available

CVE ID: CVE-2024-56611
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm/mempolicy: fix migra
Mitigation: No fix available

CVE ID: CVE-2024-56641
Description: In the Linux kernel, the following vulnerability has been resolved:■■net/smc: initialize close_w
Mitigation: No fix available

CVE ID: CVE-2024-56647
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: Fix icmp host relooku
Mitigation: No fix available

CVE ID: CVE-2024-56657
Description: In the Linux kernel, the following vulnerability has been resolved:■■ALSA: control: Avoid WA
Mitigation: No fix available

CVE ID: CVE-2024-56692
Description: In the Linux kernel, the following vulnerability has been resolved:■■f2fs: fix to do sanity check
Mitigation: No fix available

CVE ID: CVE-2024-56703
Description: In the Linux kernel, the following vulnerability has been resolved:■■ipv6: Fix soft lockups in fi
Mitigation: No fix available

CVE ID: CVE-2024-56712
Description: In the Linux kernel, the following vulnerability has been resolved:■■udmabuf: fix memory leak
Mitigation: No fix available

CVE ID: CVE-2024-56719
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: stmmac: fix TSO DM
Mitigation: No fix available

CVE ID: CVE-2024-56729
Description: In the Linux kernel, the following vulnerability has been resolved:■■smb: Initialize cfid->tcon b
Mitigation: No fix available

CVE ID: CVE-2024-56742
Description: In the Linux kernel, the following vulnerability has been resolved:■■vfio/mlx5: Fix an unwind i
Mitigation: No fix available

CVE ID: CVE-2024-56757
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: btusb: mediate
Mitigation: No fix available

CVE ID: CVE-2024-56758
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: check folio mapping
Mitigation: No fix available

CVE ID: CVE-2024-56782
Description: In the Linux kernel, the following vulnerability has been resolved:■■ACPI: x86: Add adev NUI
Mitigation: No fix available

CVE ID: CVE-2024-56786
Description: In the Linux kernel, the following vulnerability has been resolved:■■bpf: put bpf_link's prograr
Mitigation: No fix available

CVE ID: CVE-2024-57795
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/rxe: Remove the c
Mitigation: No fix available

CVE ID: CVE-2024-57802
Description: In the Linux kernel, the following vulnerability has been resolved:■■netrom: check buffer leng
Mitigation: No fix available

CVE ID: CVE-2024-57804
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: mpi3mr: Fix corrupt
Mitigation: No fix available

CVE ID: CVE-2024-57809
Description: In the Linux kernel, the following vulnerability has been resolved:■■PCI: imx6: Fix suspend/re
Mitigation: No fix available

CVE ID: CVE-2024-57841
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: fix memory leak in tc
Mitigation: No fix available

CVE ID: CVE-2024-57843
Description: In the Linux kernel, the following vulnerability has been resolved:■■virtio-net: fix overflow insi
Mitigation: No fix available

CVE ID: CVE-2024-57872
Description: In the Linux kernel, the following vulnerability has been resolved:■■scsi: ufs: pltfrm: Dellocate
Mitigation: No fix available

CVE ID: CVE-2024-57875
Description: In the Linux kernel, the following vulnerability has been resolved:■■block: RCU protect disk->
Mitigation: No fix available

CVE ID: CVE-2024-57882
Description: In the Linux kernel, the following vulnerability has been resolved:■■mptcp: fix TCP options ov
Mitigation: No fix available

CVE ID: CVE-2024-57883
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm: hugetlb: independen
Mitigation: No fix available

CVE ID: CVE-2024-57884
Description: In the Linux kernel, the following vulnerability has been resolved:■■mm: vmscan: account for
Mitigation: No fix available

CVE ID: CVE-2024-57887
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm: adv7511: Fix use-aft
Mitigation: No fix available

CVE ID: CVE-2024-57888
Description: In the Linux kernel, the following vulnerability has been resolved:■■workqueue: Do not warn
Mitigation: No fix available

CVE ID: CVE-2024-57892
Description: In the Linux kernel, the following vulnerability has been resolved:■■ocfs2: fix slab-use-after-fr
Mitigation: No fix available

CVE ID: CVE-2024-57893
Description: In the Linux kernel, the following vulnerability has been resolved:■■ALSA: seq: oss: Fix races
Mitigation: No fix available

CVE ID: CVE-2024-57895
Description: In the Linux kernel, the following vulnerability has been resolved:■■ksmbd: set ATTR_CTIME
Mitigation: No fix available

CVE ID: CVE-2024-57896
Description: In the Linux kernel, the following vulnerability has been resolved:■■btrfs: flush delalloc worke
Mitigation: No fix available

CVE ID: CVE-2024-57897
Description: In the Linux kernel, the following vulnerability has been resolved:■■drm/amdkfd: Correct the
Mitigation: No fix available

CVE ID: CVE-2024-57898
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: cfg80211: clear link I
Mitigation: No fix available

CVE ID: CVE-2024-57899
Description: In the Linux kernel, the following vulnerability has been resolved:■■wifi: mac80211: fix mbss
Mitigation: No fix available

CVE ID: CVE-2024-57900
Description: In the Linux kernel, the following vulnerability has been resolved:■■ila: serialize calls to nf_re
Mitigation: No fix available

CVE ID: CVE-2024-57902
Description: In the Linux kernel, the following vulnerability has been resolved:■■af_packet: fix vlan_get_to
Mitigation: No fix available

CVE ID: CVE-2024-57903
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: restrict SO_REUSEP
Mitigation: No fix available

CVE ID: CVE-2025-21629
Description: In the Linux kernel, the following vulnerability has been resolved:■■net: reenable NETIF_F_IP
Mitigation: No fix available

CVE ID: CVE-2004-0230
Description: TCP, when using a large Window Size, makes it easier for remote attackers to guess sequenc
Mitigation: No fix available

CVE ID: CVE-2005-3660
Description: Linux kernel 2.4 and 2.6 allows attackers to cause a denial of service (memory exhaustion an
Mitigation: No fix available

CVE ID: CVE-2007-3719
Description: The process scheduler in the Linux kernel 2.6.16 gives preference to "interactive" processes t
Mitigation: No fix available

CVE ID: CVE-2008-2544
Description: Mounting /proc filesystem via chroot command silently mounts it in read-write mode. The user
Mitigation: No fix available

CVE ID: CVE-2008-4609
Description: The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Window
Mitigation: No fix available

CVE ID: CVE-2010-4563
Description: The Linux kernel, when using IPv6, allows remote attackers to determine whether a host is sn
Mitigation: No fix available

CVE ID: CVE-2010-5321
Description: Memory leak in drivers/media/video/videobuf-core.c in the videobuf subsystem in the Linux ke
Mitigation: No fix available

CVE ID: CVE-2011-4915
Description: fs/proc/base.c in the Linux kernel through 3.1 allows local users to obtain sensitive keystroke i
Mitigation: No fix available

CVE ID: CVE-2011-4916
Description: Linux kernel through 3.1 allows local users to obtain sensitive keystroke information via acces
Mitigation: No fix available

CVE ID: CVE-2011-4917
Description: In the Linux kernel through 3.1 there is an information disclosure issue via /proc/stat.
Mitigation: No fix available

CVE ID: CVE-2012-4542
Description: block/scsi_ioctl.c in the Linux kernel through 3.8 does not properly consider the SCSI device c
Mitigation: No fix available

CVE ID: CVE-2014-9892
Description: The snd_compr_tstamp function in sound/core/compress_offload.c in the Linux kernel through
Mitigation: No fix available

CVE ID: CVE-2014-9900
Description: The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in A
Mitigation: No fix available

CVE ID: CVE-2015-2877
Description: Kernel Samepage Merging (KSM) in the Linux kernel 2.6.32 through 4.x does not prevent use
Mitigation: No fix available

CVE ID: CVE-2016-10723
Description: An issue was discovered in the Linux kernel through 4.17.2. Since the page allocator does no
Mitigation: No fix available

CVE ID: CVE-2016-8660
Description: The XFS subsystem in the Linux kernel through 4.8.2 allows local users to cause a denial of s
Mitigation: No fix available

CVE ID: CVE-2017-0630
Description: An information disclosure vulnerability in the kernel trace subsystem could enable a local mali
Mitigation: No fix available

CVE ID: CVE-2017-13693
Description: The acpi_ds_create_operands() function in drivers/acpi/acpica/dsutils.c in the Linux kernel thr
Mitigation: No fix available

CVE ID: CVE-2017-13694
Description: The acpi_ps_complete_final_op() function in drivers/acpi/acpica/psobject.c in the Linux kernel
Mitigation: No fix available

CVE ID: CVE-2018-1121
Description: procps-ng, procps is vulnerable to a process hiding through race condition. Since the kernel's
Mitigation: No fix available

CVE ID: CVE-2018-12928
Description: In the Linux kernel 4.15.0, a NULL pointer dereference was discovered in hfs_ext_read_exten
Mitigation: No fix available

CVE ID: CVE-2018-17977
Description: The Linux kernel 4.14.67 mishandles certain interaction among XFRM Netlink messages, IPP
Mitigation: No fix available

CVE ID: CVE-2019-11191
Description: The Linux kernel through 5.0.7, when CONFIG_IA32_AOUT is enabled and ia32_aout is load
Mitigation: No fix available

CVE ID: CVE-2019-12378
Description: An issue was discovered in ip6_ra_control in net/ipv6/ipv6_sockglue.c in the Linux kernel thro
Mitigation: No fix available

CVE ID: CVE-2019-12379
Description: An issue was discovered in con_insert_unipair in drivers/tty/vt/consolemap.c in the Linux kern
Mitigation: No fix available

CVE ID: CVE-2019-12380
Description: **DISPUTED** An issue was discovered in the efi subsystem in the Linux kernel through 5.1.5
Mitigation: No fix available

CVE ID: CVE-2019-12381
Description: An issue was discovered in ip_ra_control in net/ipv4/ip_sockglue.c in the Linux kernel through
Mitigation: No fix available

CVE ID: CVE-2019-12382
Description: An issue was discovered in drm_load_edid_firmware in drivers/gpu/drm/drm_edid_load.c in th
Mitigation: No fix available

CVE ID: CVE-2019-12455
Description: An issue was discovered in sunxi_divs_clk_setup in drivers/clk/sunxi/clk-sunxi.c in the Linux k
Mitigation: No fix available

CVE ID: CVE-2019-12456
Description: An issue was discovered in the MPT3COMMAND case in _ctl_ioctl_main in drivers/scsi/mpt3s
Mitigation: No fix available

CVE ID: CVE-2019-16229
Description: drivers/gpu/drm/amd/amdkfd/kfd_interrupt.c in the Linux kernel 5.2.14 does not check the allo
Mitigation: No fix available

CVE ID: CVE-2019-16230
Description: drivers/gpu/drm/radeon/radeon_display.c in the Linux kernel 5.2.14 does not check the alloc_
Mitigation: No fix available

CVE ID: CVE-2019-16231
Description: drivers/net/fjes/fjes_main.c in the Linux kernel 5.2.14 does not check the alloc_workqueue ret
Mitigation: No fix available

CVE ID: CVE-2019-16232
Description: drivers/net/wireless/marvell/libertas/if_sdio.c in the Linux kernel 5.2.14 does not check the allo
Mitigation: No fix available

CVE ID: CVE-2019-16233
Description: drivers/scsi/qla2xxx/qla_os.c in the Linux kernel 5.2.14 does not check the alloc_workqueue r
Mitigation: No fix available

CVE ID: CVE-2019-16234
Description: drivers/net/wireless/intel/iwlwifi/pcie/trans.c in the Linux kernel 5.2.14 does not check the alloc
Mitigation: No fix available

CVE ID: CVE-2019-19070
Description: A memory leak in the spi_gpio_probe() function in drivers/spi/spi-gpio.c in the Linux kernel thr
Mitigation: No fix available

CVE ID: CVE-2019-19378
Description: In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image can lead to slab-out-of-bo
Mitigation: No fix available

CVE ID: CVE-2020-11725
Description: snd_ctl_elem_add in sound/core/control.c in the Linux kernel through 5.6.3 has a count=info->
Mitigation: No fix available

CVE ID: CVE-2020-35501
Description: A flaw was found in the Linux kernels implementation of audit rules, where a syscall can unex
Mitigation: No fix available

CVE ID: CVE-2021-26934
Description: An issue was discovered in the Linux kernel 4.18 through 5.10.16, as used by Xen. The backe
Mitigation: No fix available

CVE ID: CVE-2021-3714
Description: A flaw was found in the Linux kernels memory deduplication mechanism. Previous work has s
Mitigation: No fix available

CVE ID: CVE-2022-0400
Description: An out-of-bounds read vulnerability was discovered in linux kernel in the smc protocol stack, c
Mitigation: No fix available

CVE ID: CVE-2022-1247
Description: An issue found in linux-kernel that leads to a race condition in rose_connect(). The rose driver
Mitigation: No fix available

CVE ID: CVE-2022-25265
Description: In the Linux kernel through 5.16.10, certain binary files may have the exec-all attribute if they
Mitigation: No fix available

CVE ID: CVE-2022-2961
Description: A use-after-free flaw was found in the Linux kernel’s PLP Rose functionality in the way a user
Mitigation: No fix available

CVE ID: CVE-2022-3238
Description: A double-free flaw was found in the Linux kernel’s NTFS3 subsystem in how a user triggers re
Mitigation: No fix available

CVE ID: CVE-2022-41848
Description: drivers/char/pcmcia/synclink_cs.c in the Linux kernel through 5.19.12 has a race condition and
Mitigation: No fix available

CVE ID: CVE-2022-44032
Description: An issue was discovered in the Linux kernel through 6.0.6. drivers/char/pcmcia/cm4000_cs.c
Mitigation: No fix available

CVE ID: CVE-2022-44033
Description: An issue was discovered in the Linux kernel through 6.0.6. drivers/char/pcmcia/cm4040_cs.c
Mitigation: No fix available

CVE ID: CVE-2022-44034
Description: An issue was discovered in the Linux kernel through 6.0.6. drivers/char/pcmcia/scr24x_cs.c ha
Mitigation: No fix available

CVE ID: CVE-2022-4543
Description: A flaw named "EntryBleed" was found in the Linux Kernel Page Table Isolation (KPTI). This is
Mitigation: No fix available

CVE ID: CVE-2022-45884
Description: An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvbdev.c h
Mitigation: No fix available

CVE ID: CVE-2022-45885
Description: An issue was discovered in the Linux kernel through 6.0.9. drivers/media/dvb-core/dvb_fronte
Mitigation: No fix available

CVE ID: CVE-2023-23039
Description: An issue was discovered in the Linux kernel through 6.2.0-rc2. drivers/tty/vcc.c has a race cor
Mitigation: No fix available

CVE ID: CVE-2023-26242
Description: afu_mmio_region_get_by_offset in drivers/fpga/dfl-afu-region.c in the Linux kernel through 6.1
Mitigation: No fix available

CVE ID: CVE-2023-31081
Description: An issue was discovered in drivers/media/test-drivers/vidtv/vidtv_bridge.c in the Linux kernel 6
Mitigation: No fix available

CVE ID: CVE-2023-31085
Description: An issue was discovered in drivers/mtd/ubi/cdev.c in the Linux kernel 6.2. There is a divide-by
Mitigation: No fix available

CVE ID: CVE-2023-3640
Description: A possible unauthorized memory access flaw was found in the Linux kernel's cpu_entry_area
Mitigation: No fix available

CVE ID: CVE-2023-39191
Description: An improper input validation flaw was found in the eBPF subsystem in the Linux kernel. The is
Mitigation: No fix available

CVE ID: CVE-2023-4134
Description: A use-after-free vulnerability was found in the cyttsp4_core driver in the Linux kernel. This issu
Mitigation: No fix available

CVE ID: CVE-2024-0564
Description: A flaw was found in the Linux kernel's memory deduplication mechanism. The max page shar
Mitigation: No fix available

CVE ID: CVE-2024-40918
Description: In the Linux kernel, the following vulnerability has been resolved:■■parisc: Try to fix random s
Mitigation: No fix available

CVE ID: CVE-2024-42155
Description: In the Linux kernel, the following vulnerability has been resolved:■■s390/pkey: Wipe copies o
Mitigation: No fix available

CVE ID: CVE-2024-50057
Description: In the Linux kernel, the following vulnerability has been resolved:■■usb: typec: tipd: Free IRQ
Mitigation: No fix available

CVE ID: CVE-2024-50211
Description: In the Linux kernel, the following vulnerability has been resolved:■■udf: refactor inode_bmap
Mitigation: No fix available

CVE ID: TEMP-0000000-F7A20F
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2024-54031
Description: In the Linux kernel, the following vulnerability has been resolved:■■netfilter: nft_set_hash: un
Mitigation: No fix available

CVE ID: CVE-2024-57857
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/siw: Remove direc
Mitigation: No fix available

CVE ID: CVE-2024-57889
Description: In the Linux kernel, the following vulnerability has been resolved:■■pinctrl: mcp23s08: Fix sle
Mitigation: No fix available

CVE ID: CVE-2024-57890
Description: In the Linux kernel, the following vulnerability has been resolved:■■RDMA/uverbs: Prevent in
Mitigation: No fix available

CVE ID: CVE-2024-57894
Description: In the Linux kernel, the following vulnerability has been resolved:■■Bluetooth: hci_core: Fix s
Mitigation: No fix available

CVE ID: CVE-2024-57901
Description: In the Linux kernel, the following vulnerability has been resolved:■■af_packet: fix vlan_get_p
Mitigation: No fix available

CVE ID: CVE-2023-4641
Description: A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the pa
Mitigation: No fix available

CVE ID: CVE-2007-5686
Description: initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows lo
Mitigation: No fix available

CVE ID: CVE-2023-29383
Description: In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID prog
Mitigation: No fix available

CVE ID: CVE-2024-56433
Description: shadow-utils (aka shadow) 4.4 through 4.17.0 establishes a default /etc/subuid behavior (e.g.,
Mitigation: No fix available

CVE ID: TEMP-0628843-DBAD28
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2008-1687
Description: The (1) maketemp and (2) mkstemp builtin functions in GNU m4 before 1.4.11 do not quote th
Mitigation: No fix available

CVE ID: CVE-2008-1688
Description: Unspecified vulnerability in GNU m4 before 1.4.11 might allow context-dependent attackers to
Mitigation: No fix available

CVE ID: CVE-2024-21096
Description: Vulnerability in the MySQL Server product of Oracle MySQL (component: Client: mysqldump)
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2023-50495
Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n
Mitigation: No fix available

CVE ID: CVE-2023-50495
Description: NCurse v6.4-20230418 was discovered to contain a segmentation fault via the component _n
Mitigation: No fix available

CVE ID: CVE-2007-2243
Description: OpenSSH 4.6 and earlier, when ChallengeResponseAuthentication is enabled, allows remote
Mitigation: No fix available

CVE ID: CVE-2007-2768
Description: OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote att
Mitigation: No fix available

CVE ID: CVE-2008-3234
Description: sshd in OpenSSH 4 on Debian GNU/Linux, and the 20070303 OpenSSH snapshot, allows rem
Mitigation: No fix available

CVE ID: CVE-2016-20012
Description: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combinati
Mitigation: No fix available

CVE ID: CVE-2018-15919
Description: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by rem
Mitigation: No fix available

CVE ID: CVE-2019-6110
Description: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a ma
Mitigation: No fix available

CVE ID: CVE-2020-14145
Description: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an info
Mitigation: No fix available

CVE ID: CVE-2020-15778
Description: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as d
Mitigation: No fix available

CVE ID: CVE-2023-51767
Description: OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer atta
Mitigation: No fix available

CVE ID: CVE-2023-4641
Description: A flaw was found in shadow-utils. When asking for a new password, shadow-utils asks the pa
Mitigation: No fix available

CVE ID: CVE-2007-5686
Description: initscripts in rPath Linux 1 sets insecure permissions for the /var/log/btmp file, which allows loc
Mitigation: No fix available

CVE ID: CVE-2023-29383
Description: In Shadow 4.13, it is possible to inject control characters into fields provided to the SUID prog
Mitigation: No fix available

CVE ID: CVE-2024-56433
Description: shadow-utils (aka shadow) 4.4 through 4.17.0 establishes a default /etc/subuid behavior (e.g.,
Mitigation: No fix available

CVE ID: TEMP-0628843-DBAD28
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2010-4651
Description: Directory traversal vulnerability in util.c in GNU patch 2.6.1 and earlier allows user-assisted re
Mitigation: No fix available

CVE ID: CVE-2018-6951
Description: An issue was discovered in GNU patch through 2.7.6. There is a segmentation fault, associate
Mitigation: No fix available

CVE ID: CVE-2018-6952
Description: A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.
Mitigation: No fix available

CVE ID: CVE-2021-45261
Description: An Invalid Pointer vulnerability exists in GNU patch 2.7 via the another_hunk function, which c
Mitigation: No fix available

CVE ID: CVE-2023-31484
Description: CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HT
Mitigation: No fix available

CVE ID: CVE-2011-4116
Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.
Mitigation: No fix available

CVE ID: CVE-2023-31486
Description: HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN
Mitigation: No fix available

CVE ID: CVE-2023-31484
Description: CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HT
Mitigation: No fix available

CVE ID: CVE-2011-4116
Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.
Mitigation: No fix available

CVE ID: CVE-2023-31486
Description: HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN
Mitigation: No fix available

CVE ID: CVE-2023-31484
Description: CPAN.pm before 2.35 does not verify TLS certificates when downloading distributions over HT
Mitigation: No fix available

CVE ID: CVE-2011-4116
Description: _is_safe in the File::Temp module for Perl does not properly handle symlinks.
Mitigation: No fix available

CVE ID: CVE-2023-31486
Description: HTTP::Tiny before 0.083, a Perl core module since 5.13.9 and available standalone on CPAN
Mitigation: No fix available

CVE ID: CVE-2023-4016
Description: Under some circumstances, this weakness allows a user who has access to run the “ps” utility
Mitigation: No fix available

CVE ID: CVE-2024-46901
Description: Insufficient validation of filenames against control characters in Apache Subversion repositorie
Mitigation: No fix available

CVE ID: TEMP-0517018-A83CE6
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2005-2541
Description: Tar 1.15.1 does not properly warn the user when extracting setuid or setgid files, which may a
Mitigation: No fix available

CVE ID: TEMP-0290435-0B57B5
Description: N/A
Mitigation: No fix available

CVE ID: CVE-2021-35331
Description: In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a craft
Mitigation: No fix available

CVE ID: CVE-2021-35331
Description: In Tcl 8.6.11, a format string vulnerability in nmakehlp.c might allow code execution via a craft
Mitigation: No fix available

CVE ID: CVE-2021-4217
Description: A flaw was found in unzip. The vulnerability occurs due to improper handling of Unicode string
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2022-0563
Description: A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support.
Mitigation: No fix available

CVE ID: CVE-2024-38428
Description: url.c in GNU Wget through 1.24.5 mishandles semicolons in the userinfo subcomponent of a U
Mitigation: No fix available

CVE ID: CVE-2021-31879
Description: GNU Wget through 1.21.1 does not omit the Authorization header upon a redirect to a differen
Mitigation: No fix available

CVE ID: CVE-2024-10524
Description: Applications that use Wget to access a remote resource using shorthand URLs and pass arbi
Mitigation: No fix available

CVE ID: CVE-2023-45853
Description: MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in
Mitigation: No fix available

CVE ID: CVE-2023-45853
Description: MiniZip in zlib through 1.3 has an integer overflow and resultant heap-based buffer overflow in
Mitigation: No fix available