Fixing CVEs in Debian

Almost Everything You Need to Know

Based on samueloph's presentation at DebConf 24

Agenda

i.e. what we are talking about today

1. Introductions
2. Debian Project
3. CVEs
4. CVEs for Debian
5. Fixing CVEs
6. Tips & Examples
7. Q&A

Who Am I?

Charles

- Computer Engineer
  - Ganesh
  - Gelos
- Debian Contributor
  - Packaging
  - Localization
  - Debian Developer (DD)
- Software Engineer at Toradex

Who Are You?

Who Are You?

- A few questions:
  1. Is this your first time hearing about Debian?
  2. Have you ever used/installed Debian?
  3. Do you know what CVEs are?
  4. Have you seen a CVE?
  5. Do you know how Debian fixes CVEs?

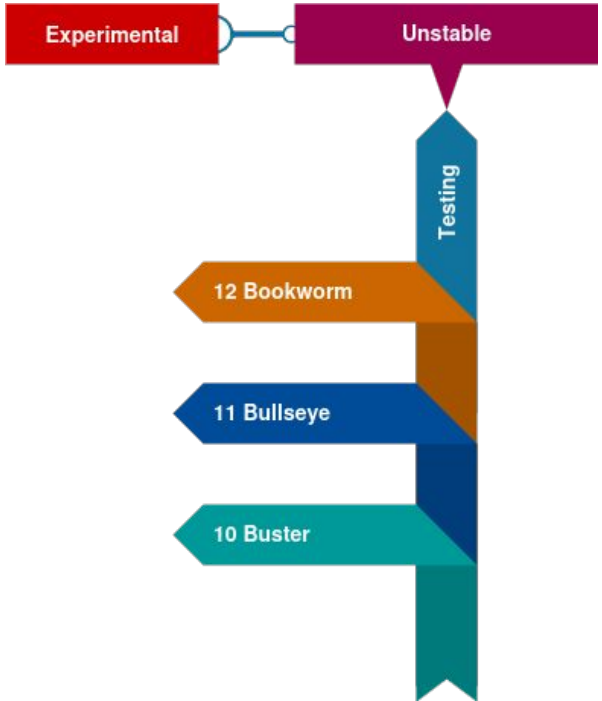
The Debian Project

About Debian :-)

- Free Software
  - Social Contract
  - Debian Free Software Guidelines
    - DFSG
- Collaborative Project
  - Constitution
  - Volunteer Based
- Transparency
  - Infrastructure
  - Mailing Lists and IRC

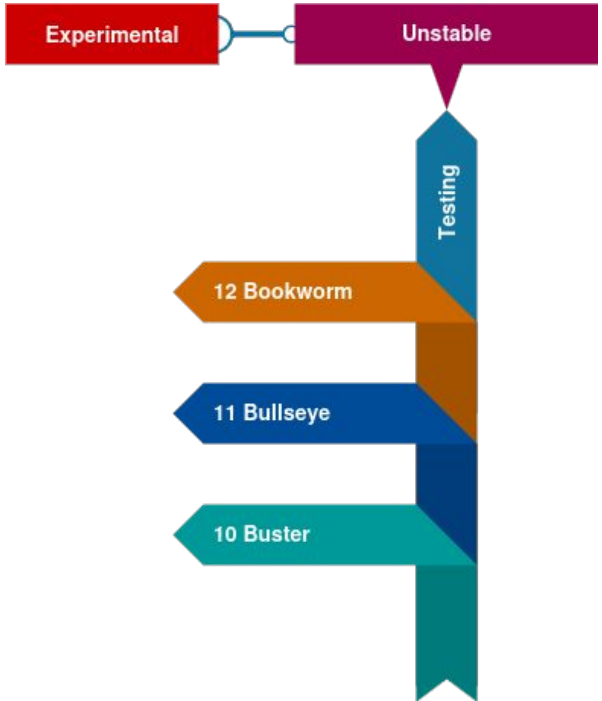
Development Cycle

- Goal:
  - Release a stable version
- How?
  - Freezing development
- The many “distros”
  - **Unstable** - Sid
    - **Experimental** - RC-Buggy
  - **Testing** - Soon to be stable
  - **Stable** - Official
  - **Oldstable** - Old



Becoming Stable

- Freeze *Testing*
  1. Toolchain
  2. Packages w/o tests
  3. All packages
- When is it released?
  - “When it’s ready”
  - **R**elease **C**ritical bugs solved
- Usually, 6 months of freezing



CVE:
Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures

- CVE ID
  - Global identifier for vulnerabilities
- Format
  - CVE-YYYY-NNNNN
- Crowdsourced effort
- Main data source worldwide
- Mutable
- Can contain misleading information

CVE-2024-7264 PUBLISHED View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Curl –

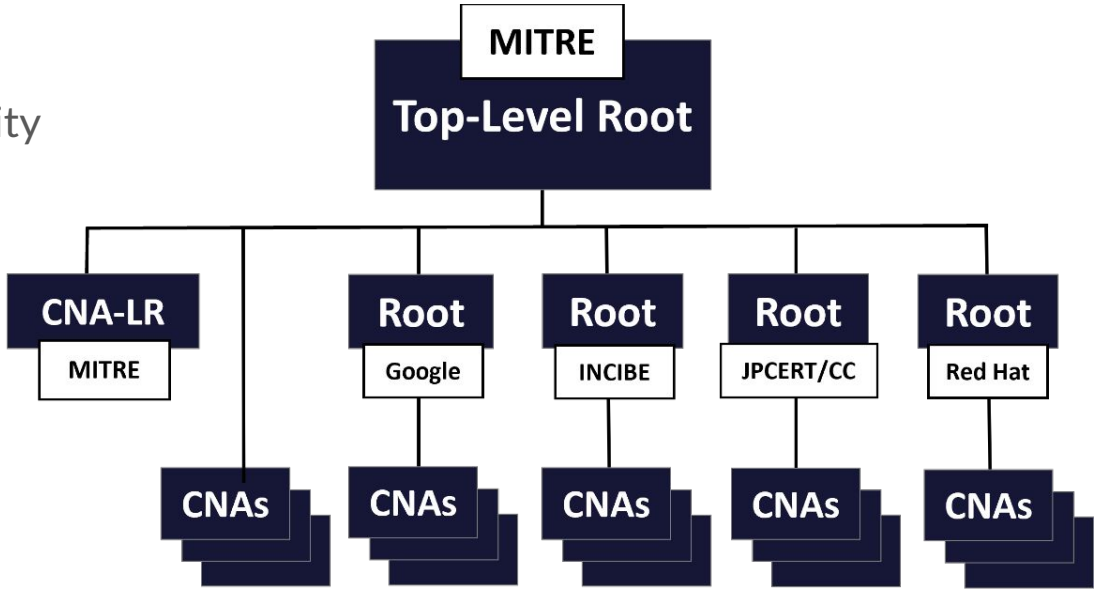
Published: 2024-07-31 **Updated:** 2024-08-02
Title: ASN.1 Date Parser Overread

Description

libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcurl/c/CURLINFO_CERTINFO.html) is used.

How can I get a CVE?

- Via CNA
  - CVE Numbering Authority
  - Hierarchical system
  - Root CNA is MITRE
  - Grouping/sub-CNAs
  - Pool of CVE IDs
  - Grant as see fit
  - Can be disputed
- cve.org at Mitre



CVEs for Debian

Security Tracker

- security-tracker.debian.org
  - Website and git repo
  - Constantly updates CVE list
  - ~80 new CVEs daily (2023)
  - From Mitre, distros@openwall and mail (team@security.d.o)
- Needs evaluation and call to action
- Can be fixed by anyone
- Security Team might issue a DSA
  - Debian Security Advisory

[SECURITY] [DSA 5587-1] curl security update

- *To*: debian-security-announce@lists.debian.org
- *Subject*: [SECURITY] [DSA 5587-1] curl security update
- *From*: Moritz Muehlenhoff <jmm@debian.org>
- *Date*: Sat, 23 Dec 2023 19:13:59 +0000

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

- ------------------------------------------------------------------------
Debian Security Advisory DSA-5587-1                   security@debian.org
https://www.debian.org/security/                       Moritz Muehlenhoff
December 23, 2023                      https://www.debian.org/security/faq
- ------------------------------------------------------------------------

Package        : curl
CVE ID         : CVE-2023-46218 CVE-2023-46219

Two security issues were discovered in Curl: Cookies were incorrectly
validated against the public suffix list of domains and in same cases
HSTS data could fail to save to disk.

For the oldstable distribution (bullseye), these problems have been fixed
in version 7.74.0-1.3+deb11u11.

For the stable distribution (bookworm), these problems have been fixed in
version 7.88.1-10+deb12u5.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to
its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian Security Advisories, how to apply
these updates to your system and frequently asked questions can be
found at: https://www.debian.org/security/

Mailing list: debian-security-announce@lists.debian.org
-----BEGIN PGP SIGNATURE-----
```

Security Team

- 3 options for CVEs
  - Apply fix and release DSA
    - Security feed
    - Embargoed (?)
  - Document and contact Maintainer
    - Proposed updates
    - Public - BTS and Infrastructure
  - Do nothing
    - Document
- Fixed with “backporting” changes

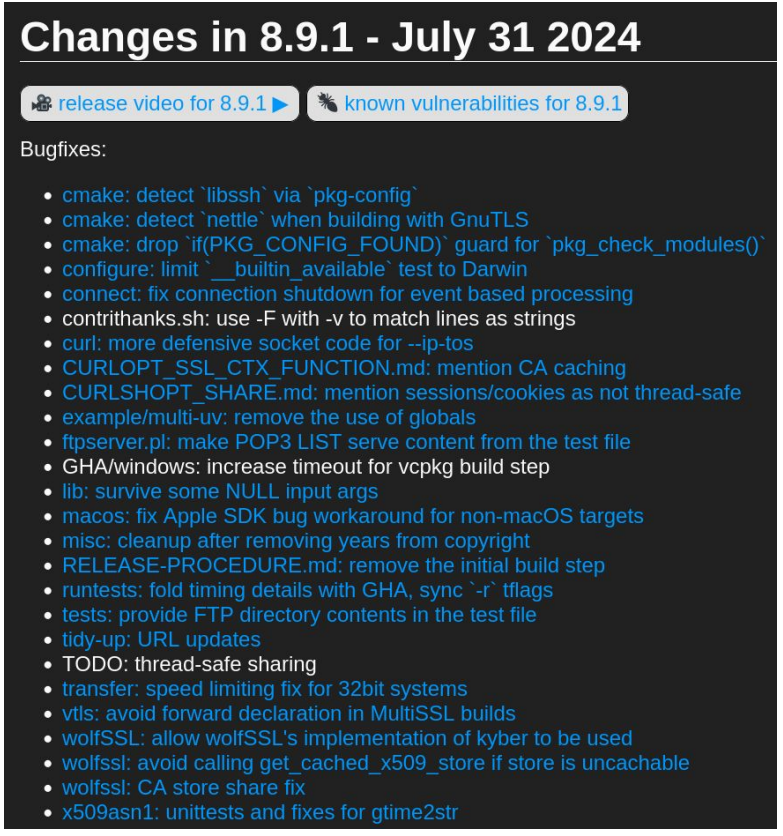
Notes

```
[bookworm] - curl <no-dsa> (Minor issue)
[bullseye] - curl <no-dsa> (Minor issue)
https://curl.se/docs/CVE-2024-7264.html
Introduced by: https://github.com/curl/curl/c
Fixed by: https://github.com/curl/curl/commit
```

Fixing CVEs

Different Views

- Upstream
  - Fix the issues
    - New major release
    - Minor/Patch release
    - Complete documentation
- Debian
  - Older version
  - Freezed in time
  - Backport the patches
    - New **Debian** release (+deb12u1)



Changes in 8.9.1 - July 31 2024

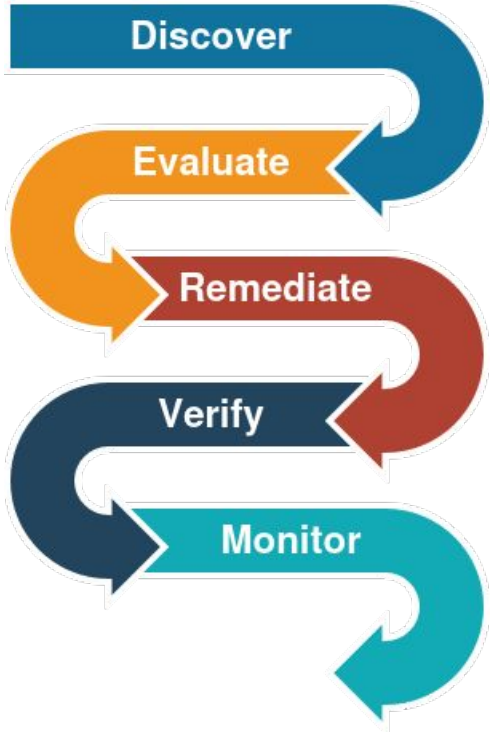
release video for 8.9.1 ▶ | known vulnerabilities for 8.9.1

Bugfixes:

- cmake: detect `libssh` via `pkg-config`
- cmake: detect `nettle` when building with GnuTLS
- cmake: drop `if(PKG_CONFIG_FOUND)` guard for `pkg_check_modules()`
- configure: limit `__builtin_available` test to Darwin
- connect: fix connection shutdown for event based processing
- contrithanks.sh: use -F with -v to match lines as strings
- curl: more defensive socket code for --ip-tos
- CURLOPT_SSL_CTX_FUNCTION.md: mention CA caching
- CURLSHOPT_SHARE.md: mention sessions/cookies as not thread-safe
- example/multi-uv: remove the use of globals
- ftpserver.pl: make POP3 LIST serve content from the test file
- GHA/windows: increase timeout for vcpkg build step
- lib: survive some NULL input args
- macos: fix Apple SDK bug workaround for non-macOS targets
- misc: cleanup after removing years from copyright
- RELEASE-PROCEDURE.md: remove the initial build step
- runtests: fold timing details with GHA, sync `-r` tflags
- tests: provide FTP directory contents in the test file
- tidy-up: URL updates
- TODO: thread-safe sharing
- transfer: speed limiting fix for 32bit systems
- vtls: avoid forward declaration in MultiSSL builds
- wolfSSL: allow wolfSSL's implementation of kyber to be used
- wolfssl: avoid calling get_cached_x509_store if store is uncachable
- wolfssl: CA store share fix
- x509asn1: unittests and fixes for gtime2str

The Process

- Find a CVE to fix
- Confirm impact
- Identify the fix
  - Apply the patches
  - Modify the patch
  - Document changes
- Review backporting changes
- Test the changes
- Submit the fixed package
- Watch for regressions



Tips & Examples

Evaluation Phase

- Understand what's going on
- Read external discussions
  - Oss-security @ openwall
- Does it depend on a feature that's not present in the build we ship?
- Does hardening blocks the exploitation?
- Which Debian releases are affected?
  - Could the vulnerability have been backported?
- Affected code bundled into another package?
- Don't trust the CVE description, verify!

Remediation Phase - Identify the Fix

- Have any other distro fixed it?
  - repology.org
  - Did they modify the patch?
- Recent fixes _might_ have hidden regressions
- Identify unexpected behavior changes
  - Features being removed
  - Introduction of operation limits

Remediation Phase - Apply the Patches

- Don't let your code editor format the patch
- Don’t autoremove trailing whitespaces
- Don’t replace tabs with spaces
- Split cherry-pick and backporting
  - 1 commit introducing the upstream patches
  - 1 commit backporting changes and documenting them
- Make sure the patches apply!

Remediation Phase - Modify the Patches

- A different patch might be a dependency
- Functions or variables might need to be renamed
- Introducing new upstream functions is risky
- List every backporting change in the patch header
- 1 commit exclusive for the backporting change

Remediation Phase - Review the Backport

- Backporting changes = diff of a diff
- Reviewing backporting commits saves the day
- If we release a broken fix, a new CVE is created to track it
- Pay attention to reordering of hunks
- Question everything

Verify Phase - Test the Changes

- Upstream regression tests on a later commit?
- Other distros' tests?
- Autopkgtest of a reverse-dependency?
- Proof-of-concept available?

Monitor Phase

- Mention the CVE ID and a short summary in d/changelog
- Follow the right update submission process
  - Proposed-updates process – NO-DSA
  - Security team process – DSA
- Watch the BTS for user's bug reports
- Watch for reverse dependencies tests (in all arches!)

Contact Info

- **charles** [at] debian [dot] org
- Telegram: charles_melara
- IRC: charles (oftc/libera)
- Questions or Comments?
- License: CC BY-SA 4.0

Daqui para baixo:
slides para apresentação

Fixing CVEs in Debian

Almost Everything You Need to Know

Based on samueloph's presentation at DebConf 24

Agenda

i.e. what we are talking about today

1. Introductions
2. Debian Project
3. CVEs
4. CVEs for Debian
5. Fixing CVEs
6. Tips & Examples
7. Q&A

Who Am I?

Charles

- Computer Engineer
  - Ganesh

Charles

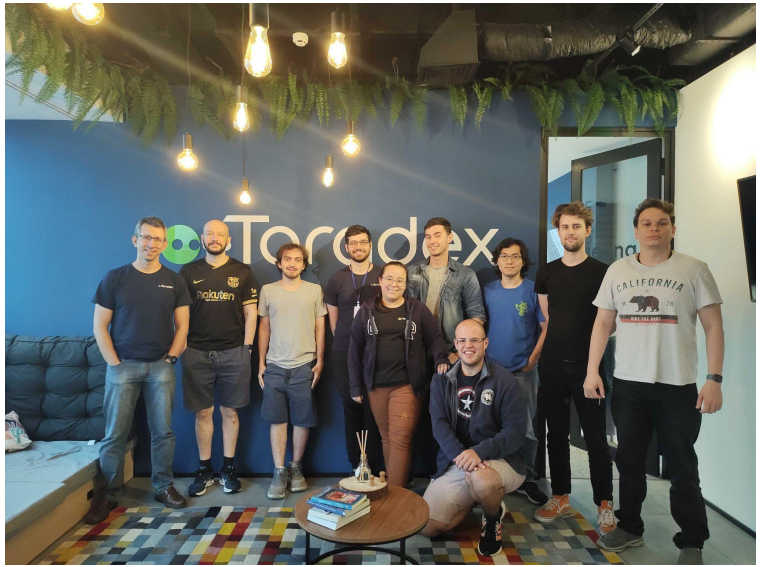
- Computer Engineer
  - Ganesh
  - Gelos

Charles

- Computer Engineer
  - Ganesh
  - Gelos
- Debian Contributor
  - Packaging
  - Localization
  - Debian Developer (DD)

Charles

- Computer Engineer
  - Ganesh
  - Gelos
- Debian Contributor
  - Packaging
  - Localization
  - Debian Developer (DD)
- Software Engineer at Toradex



Who Are You?

Who Are You?

- A few questions:
    1. Is this your first time hearing about Debian?

Who Are You?

- A few questions:
  1. Is this your first time hearing about Debian?
  2. Have you ever used/installed Debian?

Who Are You?

- A few questions:
  1. Is this your first time hearing about Debian?
  2. Have you ever used/installed Debian?
  3. Do you know what CVEs are?

Who Are You?

- A few questions:
  1. Is this your first time hearing about Debian?
  2. Have you ever used/installed Debian?
  3. Do you know what CVEs are?
  4. Have you seen a CVE?

Who Are You?

- A few questions:
  1. Is this your first time hearing about Debian?
  2. Have you ever used/installed Debian?
  3. Do you know what CVEs are?
  4. Have you seen a CVE?
  5. Do you know how Debian fixes CVEs?

The Debian Project

About Debian :-)

- Free Software
  - Social Contract
  - Debian Free Software Guidelines
    - DFSG

About Debian :-)

- Free Software
  - Social Contract
  - Debian Free Software Guidelines
    - DFSG
- Collaborative Project
  - Constitution
  - Volunteer Based

About Debian :-)

- Free Software
  - Social Contract
  - Debian Free Software Guidelines
    - DFSG
- Collaborative Project
  - Constitution
  - Volunteer Based
- Transparency
  - Infrastructure
  - Mailing Lists and IRC

Development Cycle

- Goal:
  - Release a stable version

https://www.monolitonimbus.com.br/linux-debian/ - Montagem: ViniRoger

Development Cycle

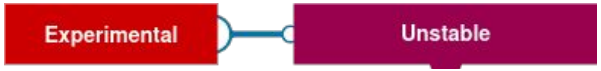
- Goal:
  - Release a stable version
- How?
  - Freezing development

https://www.monolitonimbus.com.br/linux-debian/ - Montagem: ViniRoger

Development Cycle

- Goal:
  - Release a stable version
- How?
  - Freezing development
- The many “distros”
  - **Unstable** - Sid

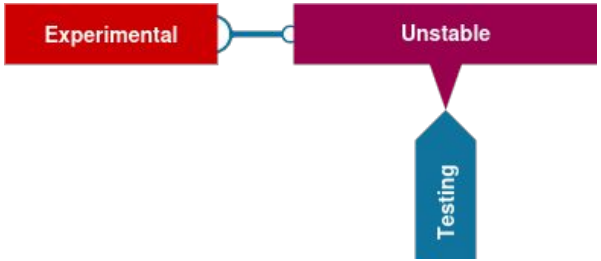
Development Cycle



- Goal:
  - Release a stable version
- How?
  - Freezing development
- The many “distros”
  - **Unstable** - Sid
    - **Experimental** - RC-Buggy

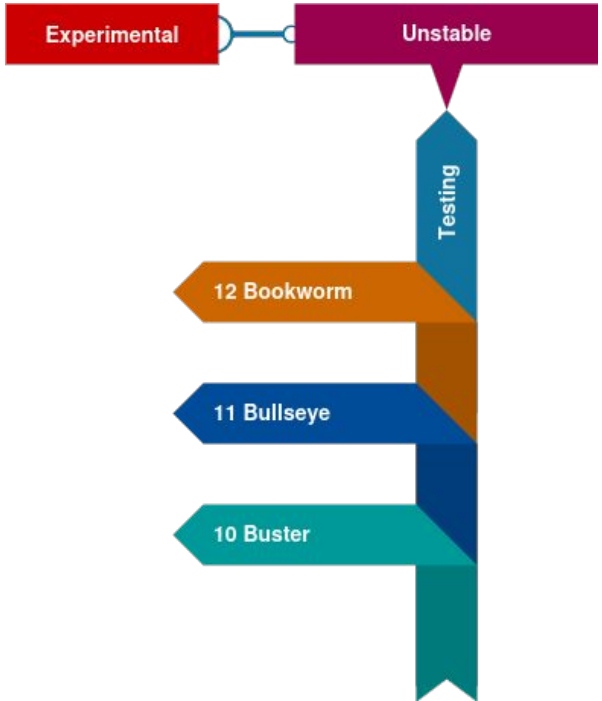
Development Cycle

- Goal:
  - Release a stable version
- How?
  - Freezing development
- The many “distros”
  - **Unstable** - Sid
    - **Experimental** - RC-Buggy
  - **Testing** - Soon to be stable



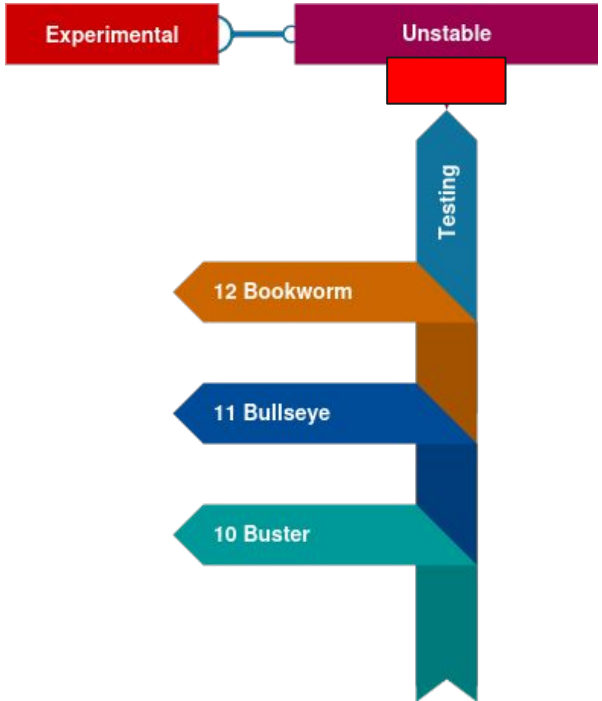
Development Cycle

- Goal:
  - Release a stable version
- How?
  - Freezing development
- The many “distros”
  - **Unstable** - Sid
    - **Experimental** - RC-Buggy
  - **Testing** - Soon to be stable
  - **Stable** - Official
  - **Oldstable** - Old



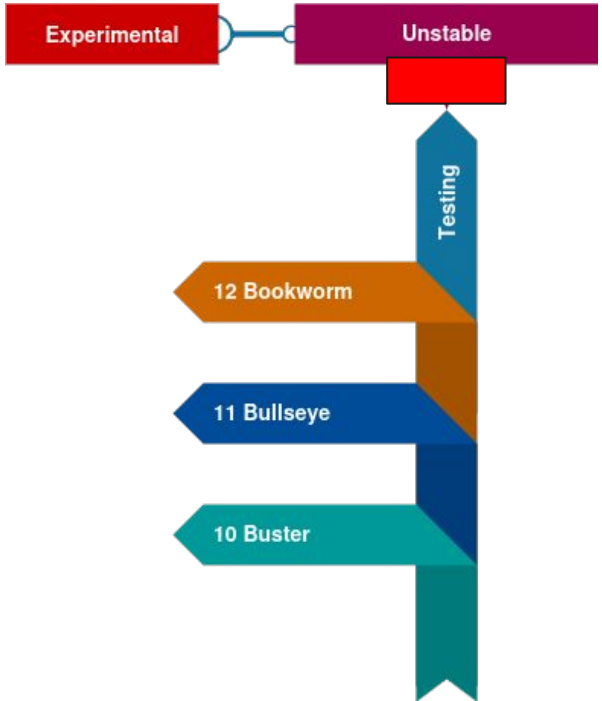
Becoming Stable

- Freeze *Testing*
  1. Toolchain
  2. Packages w/o tests
  3. All packages



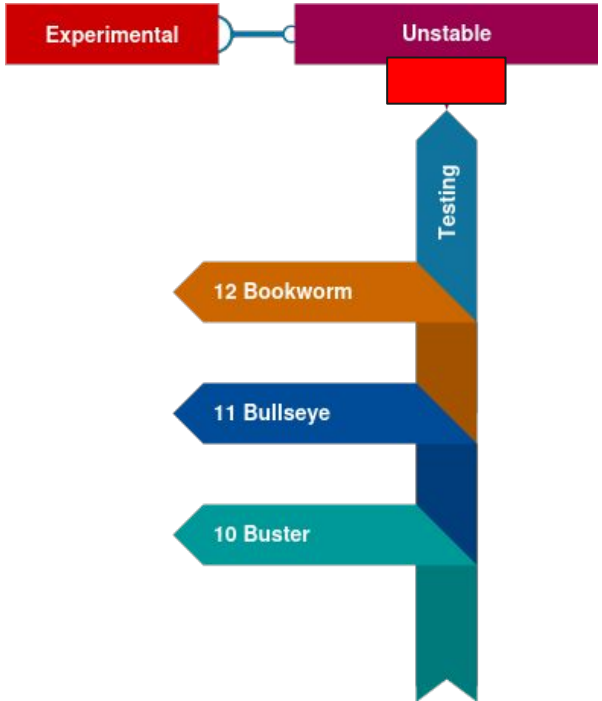
Becoming Stable

- Freeze *Testing*
  1. Toolchain
  2. Packages w/o tests
  3. All packages
- When is it released?
  - “When it’s ready”
  - **R**elease **C**ritical bugs solved



Becoming Stable

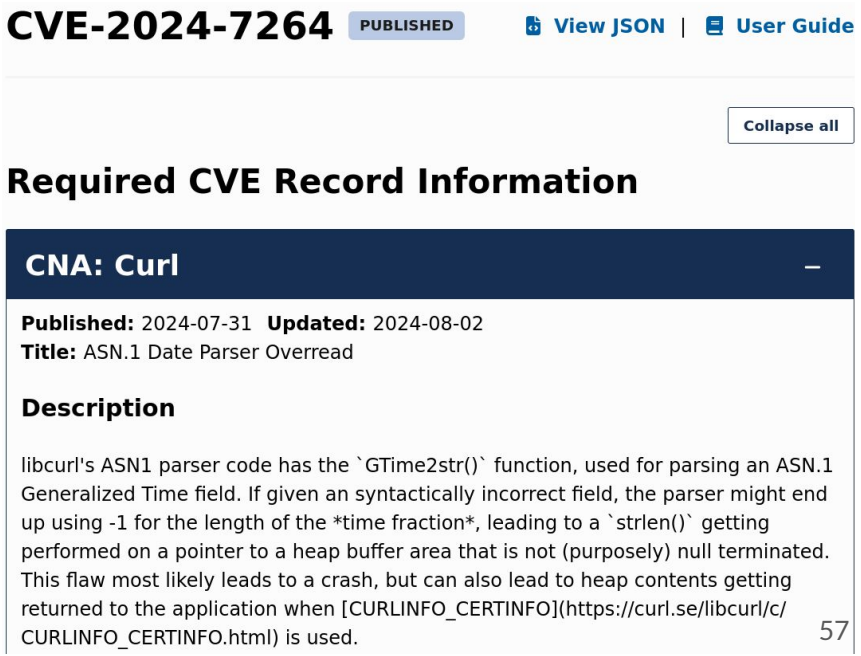
- Freeze *Testing*
  1. Toolchain
  2. Packages w/o tests
  3. All packages
- When is it released?
  - “When it’s ready”
  - **R**elease **C**ritical bugs solved
- Usually, 6 months of freezing



CVE:
Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures

- CVE ID
  - Global identifier for vulnerabilities
- Format
  - CVE-YYYY-NNNNN



CVE-2024-7264 PUBLISHED View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Curl –

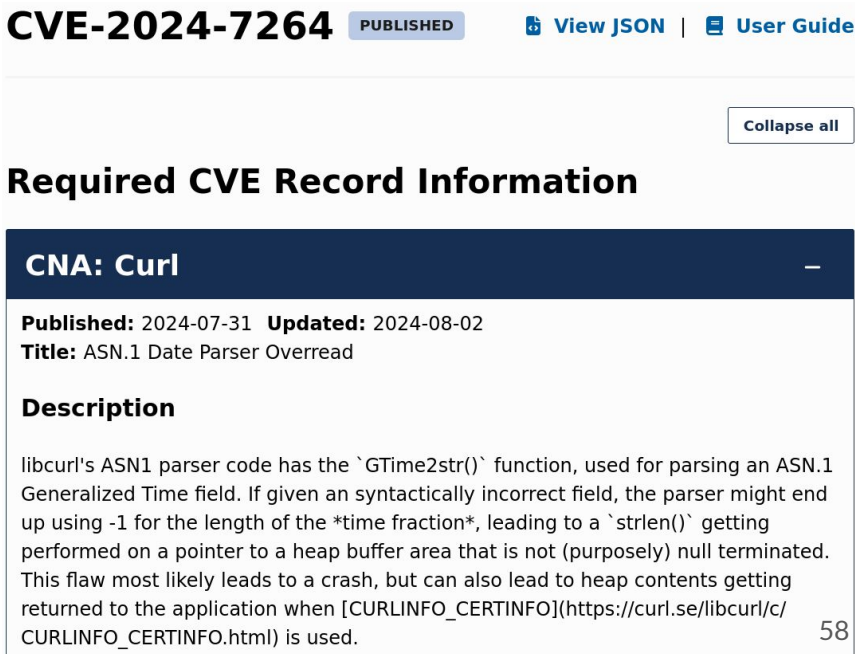
Published: 2024-07-31 **Updated:** 2024-08-02
Title: ASN.1 Date Parser Overread

Description

libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcurl/c/CURLINFO_CERTINFO.html) is used.

Common Vulnerabilities and Exposures

- CVE ID
  - Global identifier for vulnerabilities
- Format
  - CVE-YYYY-NNNNN
- Crowdsourced effort
- Main data source worldwide



CVE-2024-7264 PUBLISHED View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Curl –

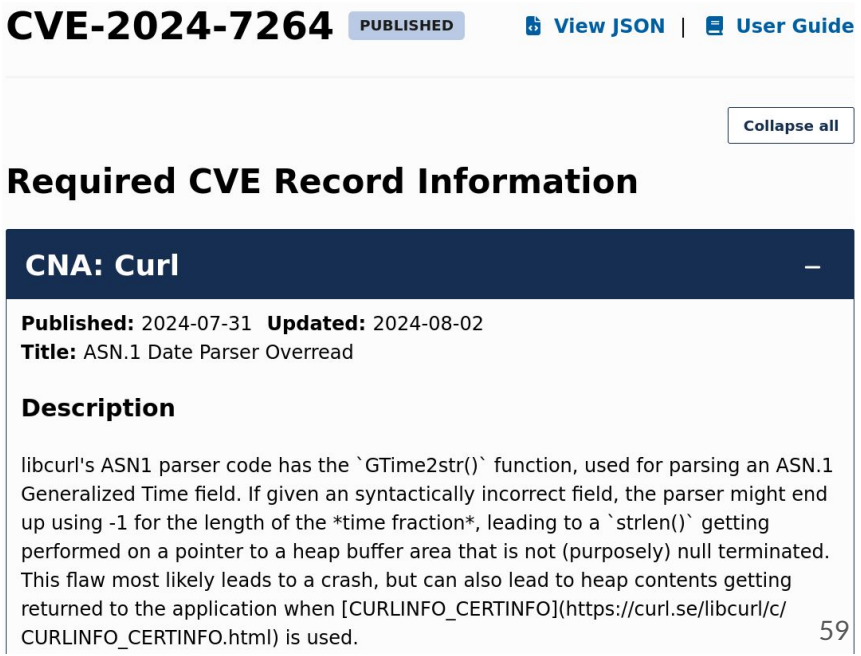
Published: 2024-07-31 **Updated:** 2024-08-02
Title: ASN.1 Date Parser Overread

Description

libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcurl/c/CURLINFO_CERTINFO.html) is used.

Common Vulnerabilities and Exposures

- CVE ID
  - Global identifier for vulnerabilities
- Format
  - CVE-YYYY-NNNNN
- Crowdsourced effort
- Main data source worldwide
- Mutable



CVE-2024-7264 PUBLISHED View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Curl –

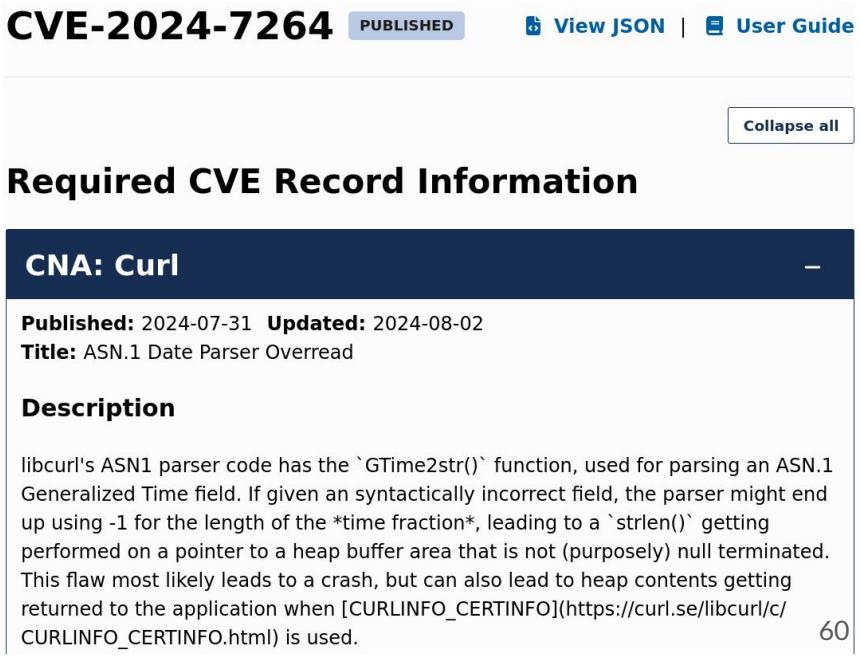
Published: 2024-07-31 **Updated:** 2024-08-02
Title: ASN.1 Date Parser Overread

Description

libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcurl/c/CURLINFO_CERTINFO.html) is used.

Common Vulnerabilities and Exposures

- CVE ID
  - Global identifier for vulnerabilities
- Format
  - CVE-YYYY-NNNNN
- Crowdsourced effort
- Main data source worldwide
- Mutable
- Can contain misleading information



CVE-2024-7264 PUBLISHED View JSON | User Guide

Collapse all

Required CVE Record Information

CNA: Curl –

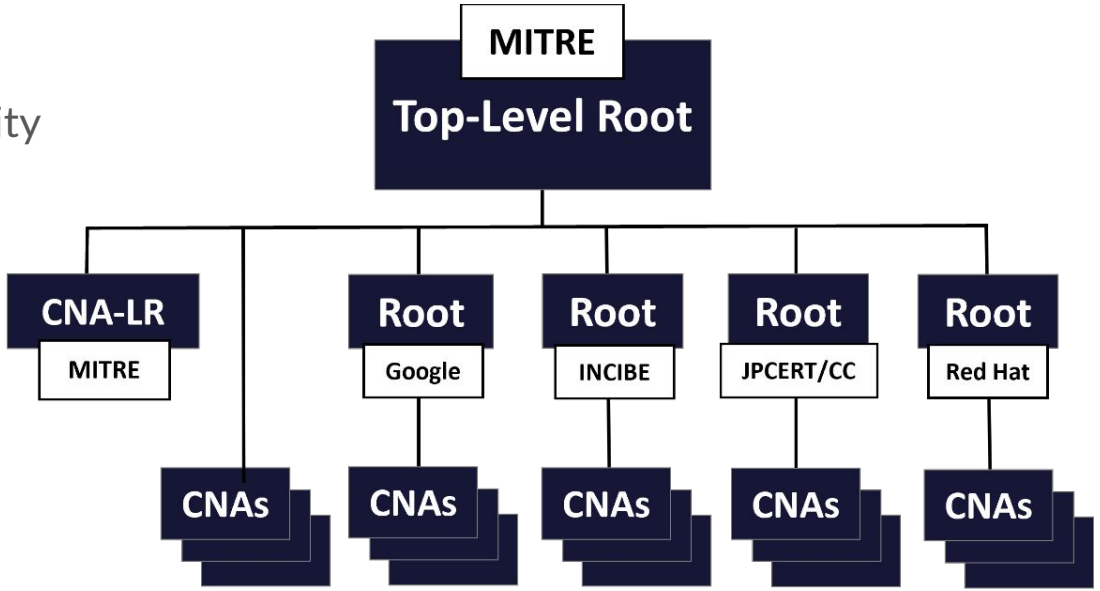
Published: 2024-07-31 **Updated:** 2024-08-02
Title: ASN.1 Date Parser Overread

Description

libcurl's ASN1 parser code has the `GTime2str()` function, used for parsing an ASN.1 Generalized Time field. If given an syntactically incorrect field, the parser might end up using -1 for the length of the *time fraction*, leading to a `strlen()` getting performed on a pointer to a heap buffer area that is not (purposely) null terminated. This flaw most likely leads to a crash, but can also lead to heap contents getting returned to the application when [CURLINFO_CERTINFO](https://curl.se/libcurl/c/CURLINFO_CERTINFO.html) is used.

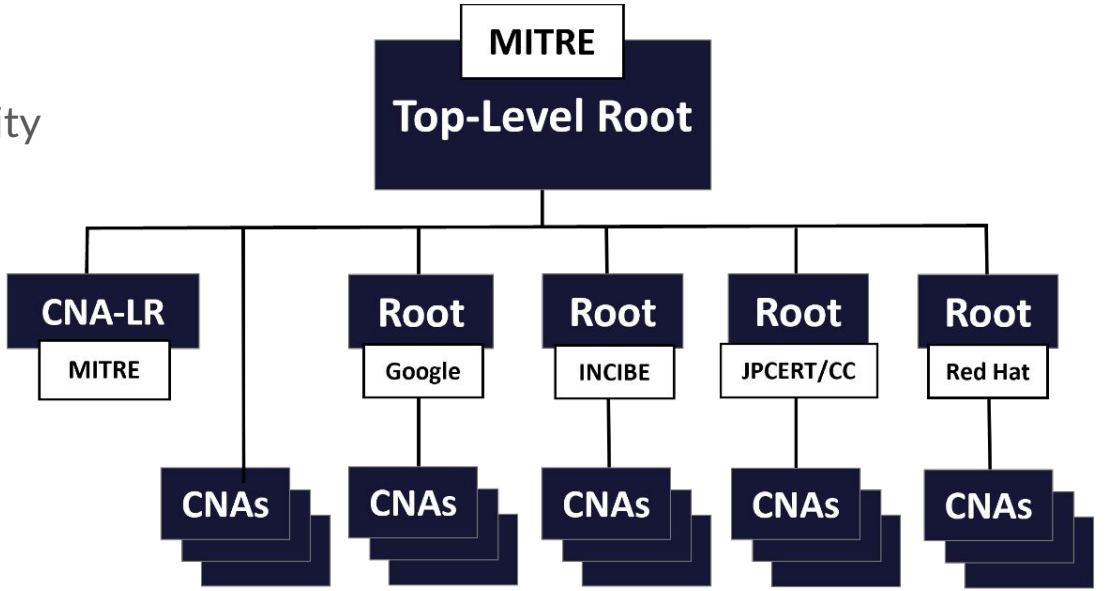
How can I get a CVE?

- Via CNA
  - CVE Numbering Authority
  - Hierarchical system
  - Root CNA is MITRE
  - Grouping/sub-CNAs
  - Pool of CVE IDs
  - Grant as see fit
  - Can be disputed



How can I get a CVE?

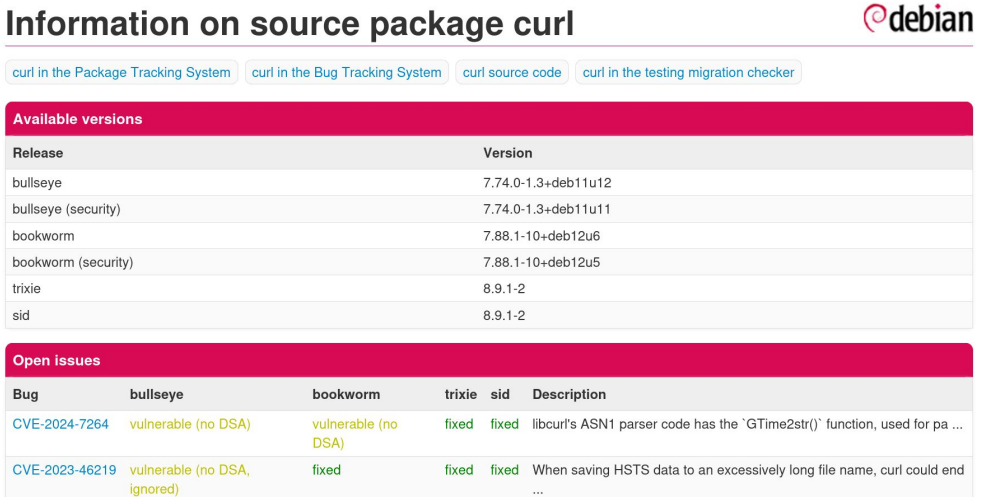
- Via CNA
  - CVE Numbering Authority
  - Hierarchical system
  - Root CNA is MITRE
  - Grouping/sub-CNAs
  - Pool of CVE IDs
  - Grant as see fit
  - Can be disputed
- cve.org at Mitre



CVEs for Debian

Security Tracker

- security-tracker.debian.org
  - Website and git repo
  - Constantly updates CVE list
  - ~80 new CVEs daily (2023)
  - From Mitre, distros@openwall and mail (team@security.d.o)



Information on source package curl

debian

curl in the Package Tracking System | curl in the Bug Tracking System | curl source code | curl in the testing migration checker

Available versions

Release	Version
bullseye	7.74.0-1.3+deb11u12
bullseye (security)	7.74.0-1.3+deb11u11
bookworm	7.88.1-10+deb12u6
bookworm (security)	7.88.1-10+deb12u5
trixie	8.9.1-2
sid	8.9.1-2

Open issues

Bug	bullseye	bookworm	trixie	sid	Description
CVE-2024-7264	vulnerable (no DSA)	vulnerable (no DSA)	fixed	fixed	libcurl's ASN1 parser code has the `GTime2str()` function, used for pa ...
CVE-2023-46219	vulnerable (no DSA, ignored)	fixed	fixed	fixed	When saving HSTS data to an excessively long file name, curl could end ...

Security Tracker

- security-tracker.debian.org
  - Website and git repo
  - Constantly updates CVE list
  - ~80 new CVEs daily (2023)
  - From Mitre, distros@openwall and mail (team@security.d.o)
- Needs evaluation and call to action
- Can be fixed by anyone

Open issues

Bug	bullseye	bookworm	trixie	sid
CVE-2024-7264	vulnerable (no DSA)	vulnerable (no DSA)	fixed	fixed
CVE-2023-46219	vulnerable (no DSA, ignored)	fixed	fixed	fixed
CVE-2023-23915	vulnerable (no DSA, ignored)	fixed	fixed	fixed
CVE-2023-23914	vulnerable (no DSA, ignored)	fixed	fixed	fixed
CVE-2022-43551	vulnerable (no DSA, ignored)	fixed	fixed	fixed
CVE-2022-42916	vulnerable (no DSA, ignored)	fixed	fixed	fixed

Open unimportant issues

Bug	bullseye	bookworm	trixie	sid	Description
CVE-2024-2379	vulnerable	vulnerable	fixed	fixed	libcurl skips the ce

Security Tracker

- security-tracker.debian.org
  - Website and git repo
  - Constantly updates CVE list
  - ~80 new CVEs daily (2023)
  - From Mitre, distros@openwall and mail (team@security.d.o)
- Needs evaluation and call to action
- Can be fixed by anyone
- Security Team might issue a DSA
  - Debian Security Advisory

[SECURITY] [DSA 5587-1] curl security update

- *To*: debian-security-announce@lists.debian.org
- *Subject*: [SECURITY] [DSA 5587-1] curl security update
- *From*: Moritz Muehlenhoff <jmm@debian.org>
- *Date*: Sat, 23 Dec 2023 19:13:59 +0000

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

- ------------------------------------------------------------------------
Debian Security Advisory DSA-5587-1                   security@debian.org
https://www.debian.org/security/                       Moritz Muehlenhoff
December 23, 2023                      https://www.debian.org/security/faq
- ------------------------------------------------------------------------

Package        : curl
CVE ID         : CVE-2023-46218 CVE-2023-46219

Two security issues were discovered in Curl: Cookies were incorrectly
validated against the public suffix list of domains and in same cases
HSTS data could fail to save to disk.

For the oldstable distribution (bullseye), these problems have been fixed
in version 7.74.0-1.3+deb11u11.

For the stable distribution (bookworm), these problems have been fixed in
version 7.88.1-10+deb12u5.

We recommend that you upgrade your curl packages.

For the detailed security status of curl please refer to
its security tracker page at:
https://security-tracker.debian.org/tracker/curl

Further information about Debian Security Advisories, how to apply
these updates to your system and frequently asked questions can be
found at: https://www.debian.org/security/

Mailing list: debian-security-announce@lists.debian.org
-----BEGIN PGP SIGNATURE-----
```

Security Team

- 3 options for CVEs
  - Apply fix and release DSA
    - Security feed
    - Embargoed (?)
  - Document and contact Maintainer
    - Proposed updates
    - Public - BTS and Infrastructure
  - Do nothing
    - Document

Notes

```
[bookworm] - curl <no-dsa> (Minor issue)
[bullseye] - curl <no-dsa> (Minor issue)
https://curl.se/docs/CVE-2024-7264.html
Introduced by: https://github.com/curl/curl/c
Fixed by: https://github.com/curl/curl/commit
```

Security Team

- 3 options for CVEs
  - Apply fix and release DSA
    - Security feed
    - Embargoed (?)
  - Document and contact Maintainer
    - Proposed updates
    - Public - BTS and Infrastructure
  - Do nothing
    - Document
- Fixed with “backporting” changes

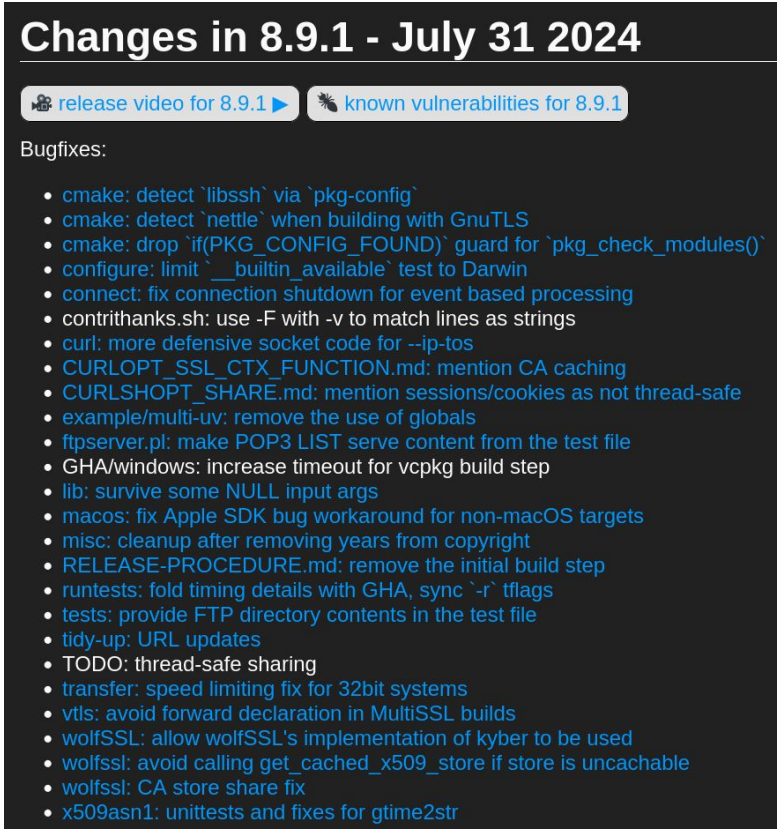
Notes

```
[bookworm] - curl <no-dsa> (Minor issue)
[bullseye] - curl <no-dsa> (Minor issue)
https://curl.se/docs/CVE-2024-7264.html
Introduced by: https://github.com/curl/curl/c
Fixed by: https://github.com/curl/curl/commit
```

Fixing CVEs

Different Views

- Upstream
  - Fix the issues
    - New major release
    - Minor/Patch release
    - Complete documentation



Changes in 8.9.1 - July 31 2024

release video for 8.9.1 ▶ | known vulnerabilities for 8.9.1

Bugfixes:

- cmake: detect `libssh` via `pkg-config`
- cmake: detect `nettle` when building with GnuTLS
- cmake: drop `if(PKG_CONFIG_FOUND)` guard for `pkg_check_modules()`
- configure: limit `__builtin_available` test to Darwin
- connect: fix connection shutdown for event based processing
- contrithanks.sh: use -F with -v to match lines as strings
- curl: more defensive socket code for --ip-tos
- CURLOPT_SSL_CTX_FUNCTION.md: mention CA caching
- CURLSHOPT_SHARE.md: mention sessions/cookies as not thread-safe
- example/multi-uv: remove the use of globals
- ftpserver.pl: make POP3 LIST serve content from the test file
- GHA/windows: increase timeout for vcpkg build step
- lib: survive some NULL input args
- macos: fix Apple SDK bug workaround for non-macOS targets
- misc: cleanup after removing years from copyright
- RELEASE-PROCEDURE.md: remove the initial build step
- runtests: fold timing details with GHA, sync `-r` tflags
- tests: provide FTP directory contents in the test file
- tidy-up: URL updates
- TODO: thread-safe sharing
- transfer: speed limiting fix for 32bit systems
- vtls: avoid forward declaration in MultiSSL builds
- wolfSSL: allow wolfSSL's implementation of kyber to be used
- wolfssl: avoid calling get_cached_x509_store if store is uncachable
- wolfssl: CA store share fix
- x509asn1: unittests and fixes for gtime2str

Different Views

- Upstream
  - Fix the issues
    - New major release
    - Minor/Patch release
    - Complete documentation
- Debian
  - Older version
  - Freezed in time
  - Backport the patches
    - New **Debian** release (+deb12u1)

package curl

curl in the Package Tracking System | curl in the Bug Tracking System | cur

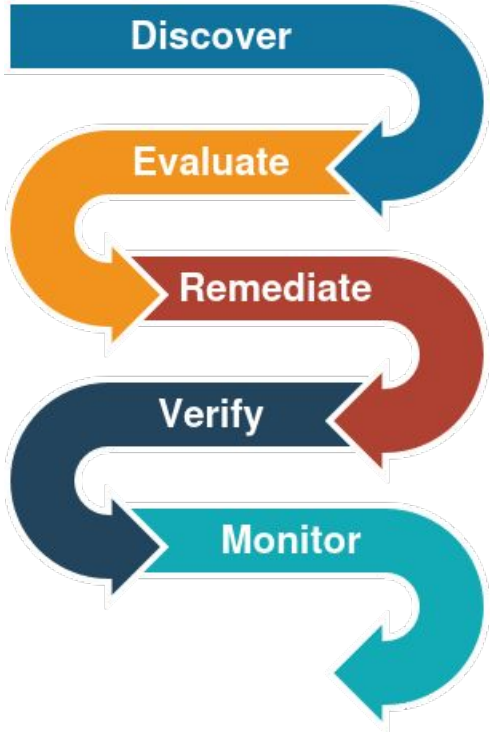
curl in the testing migration checker

Available versions

Release	Version
bullseye	7.74.0-1.3+deb11u12
bullseye (security)	7.74.0-1.3+deb11u11
bookworm	7.88.1-10+deb12u6
bookworm (security)	7.88.1-10+deb12u5
trixie	8.9.1-2
sid	8.9.1-2

The Process

- Find a CVE to fix
- Confirm impact
- Identify the fix
  - Apply the patches
  - Modify the patch
  - Document changes
- Review backporting changes
- Test the changes
- Submit the fixed package
- Watch for regressions



Tips & Examples

Evaluation Phase

- Understand what's going on
- Read external discussions
  - Oss-security @ openwall
- Does it depend on a feature that's not present in the build we ship?
- Does hardening blocks the exploitation?
- Which Debian releases are affected?
  - Could the vulnerability have been backported?
- Affected code bundled into another package?
- Don't trust the CVE description, verify!

Remediation Phase - Identify the Fix

- Have any other distro fixed it?
  - repology.org
  - Did they modify the patch?
- Recent fixes _might_ have hidden regressions
- Identify unexpected behavior changes
  - Features being removed
  - Introduction of operation limits

Remediation Phase - Apply the Patches

- Don't let your code editor format the patch
- Don’t autoremove trailing whitespaces
- Don’t replace tabs with spaces
- Split cherry-pick and backporting
  - 1 commit introducing the upstream patches
  - 1 commit backporting changes and documenting them
- Make sure the patches apply!

Remediation Phase - Modify the Patches

- A different patch might be a dependency
- Functions or variables might need to be renamed
- Introducing new upstream functions is risky
- List every backporting change in the patch header
- 1 commit exclusive for the backporting change

Remediation Phase - Review the Backport

- Backporting changes = diff of a diff
- Reviewing backporting commits saves the day
- If we release a broken fix, a new CVE is created to track it
- Pay attention to reordering of hunks
- Question everything

Verify Phase - Test the Changes

- Upstream regression tests on a later commit?
- Other distros' tests?
- Autopkgtest of a reverse-dependency?
- Proof-of-concept available?

Monitor Phase

- Mention the CVE ID and a short summary in d/changelog
- Follow the right update submission process
  - Proposed-updates process – NO-DSA
  - Security team process – DSA
- Watch the BTS for user's bug reports
- Watch for reverse dependencies tests (in all arches!)

Contact Info

- **charles** [at] debian [dot] org
- Telegram: charles_melara
- IRC: charles (oftc/libera)
- Questions or Comments?
- License: CC BY-SA 4.0