The Security of Debian

An Introduction for Advanced Users

DebConf 25

Brest, France

Slides available at samueloph.dev/slides

About me

- Samuel Henrique <samueloph>
- Debian Developer since 2018
  - Contributes on personal time, as a volunteer (not during work hours)
- Member of the Security Tools Packaging Team
- Maintains curl, rsync, shellcheck...
- Mentorship for newcomers learning packaging
- Senior System Development Engineer for Amazon Linux, Security Team
- Debian/Linux, Python, Rust, Bash, Security
- linkedin.com/in/samueloph
- samueloph.dev

Summary

- CVEs
- The Debian Support
- CVE Analysis
- Fixing CVEs
- Distributing Fixes
- Investigating It Yourself
- Common Mistakes
- Good Practices

Areas of Security

- Infrastructure
- Governance
- Package Ingestion
- Package Building
- Package Distribution
- Incident Response
- Vulnerabilities in Debian packages

Common Vulnerabilities and Exposures (CVE)

- Created in 1999 by MITRE, sponsored by the US government
  - cve.org
- Universal ID - CVE-YYYY-NNNN, e.g.: CVE-2023-4911
  - cve.org/CVERecord?id=CVE-2023-4911
- Coordination of announcements of security vulnerabilities with a public database
- Any person can report/request a CVE ID
  - cve.org/ReportRequest/ReportRequestForNonCNAs
- CVEs are enriched by other organizations through republishing
  - NVD, by NIST - Severity and Score
    - nvd.nist.gov/vuln/detail/CVE-2023-4911
  - Amazon, Debian, Ubuntu, Redhat, SUSE...
    - security-tracker.debian.org/tracker/CVE-2023-4911
    - explore.alas.aws.amazon.com/CVE-2023-4911.html
- Common Weakness Enumeration - CWE
  - cwe.mitre.org - cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html

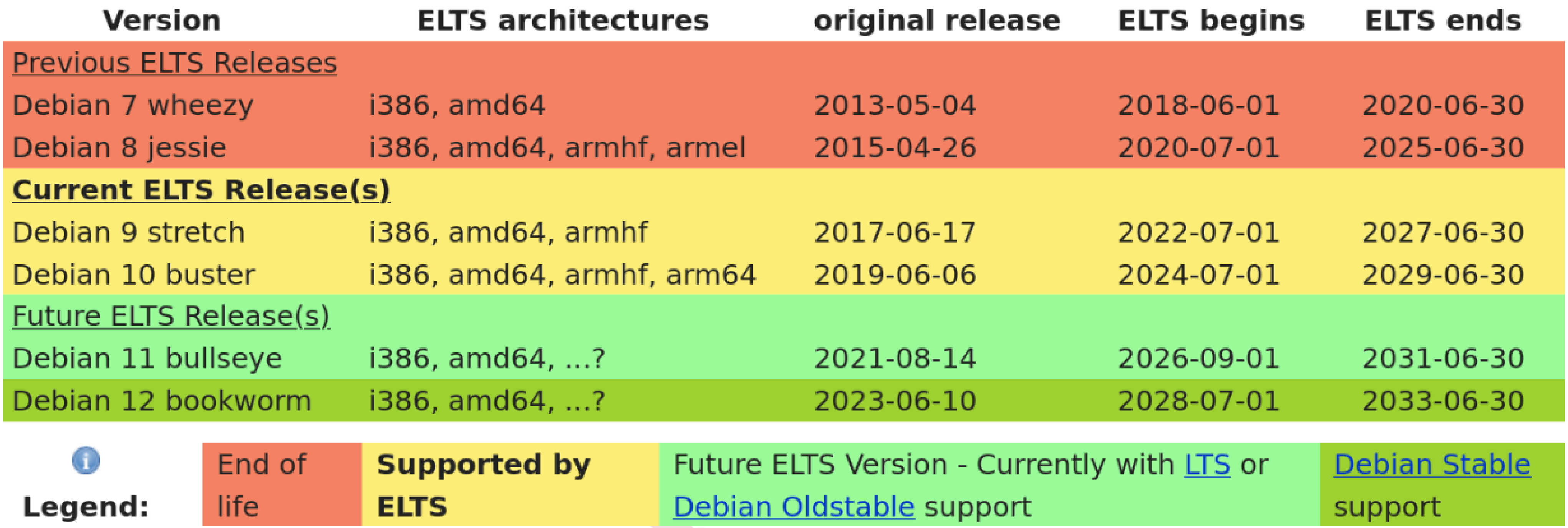
CVE Alternatives

- Github - GHSA: github.com/advisories/GHSA-m77w-6vjw-wh2f
- Distributed Weakness Filing (DWF) - Inactive
- RustSec Advisory Database - RUSTSEC-YYYY-NNNN
  - rustsec.org
- Go Vulnerability Database - GO-YYYY-NNNN
  - pkg.go.dev/vuln
- Geopolitical Entities
  - Japan
  - China
  - Russia
  - Europe - CERT-EU

The Debian Support

- 3 years by the Debian Security Team
- +2 years by the LTS Team
- +5 years by the ELTS Team
  - Support provided by the Freexian company
  - Requires usage of external repository
  - Sponsored by Freexian’s customers, but available for free to everyone
- 10 years of support in total

https://wiki.debian.org/LTS/Extended



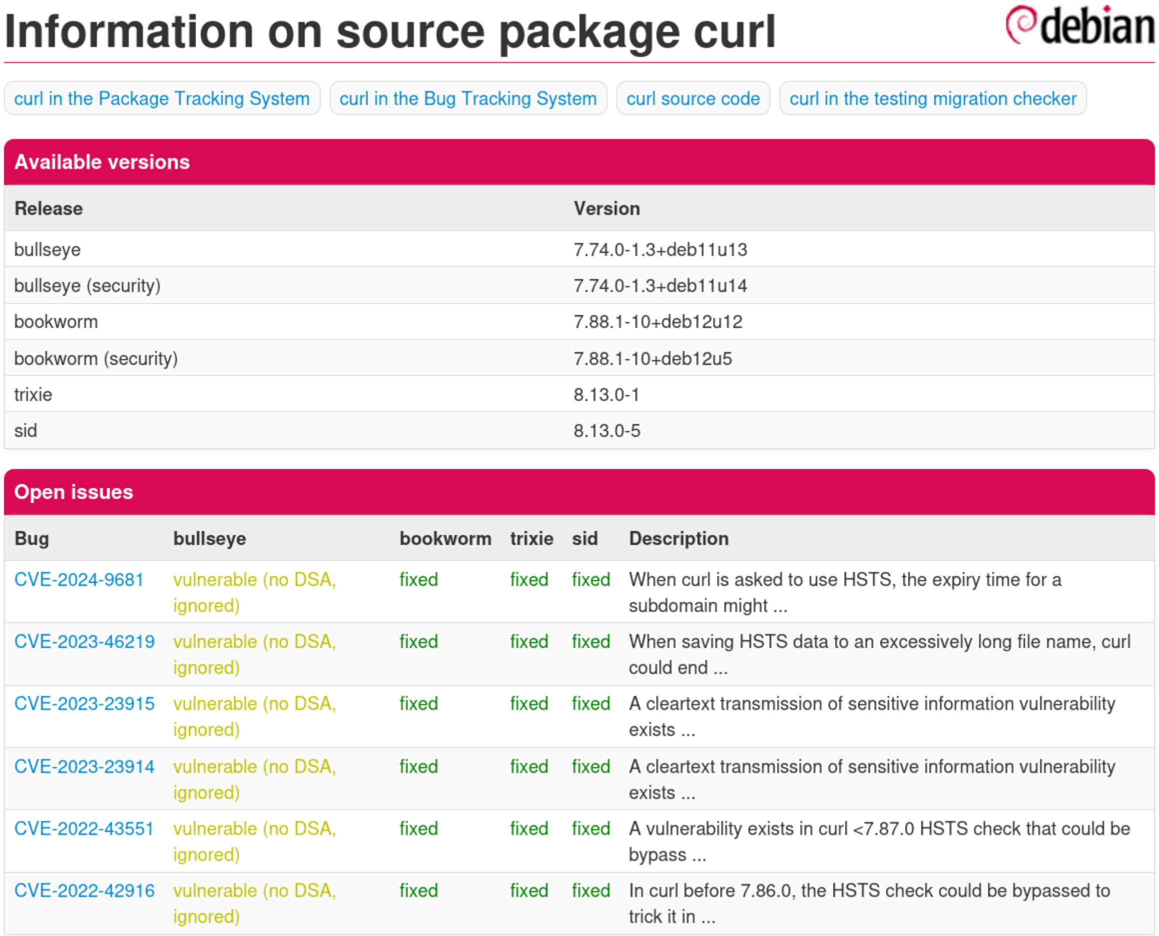
Version	ELTS architectures	original release	ELTS begins	ELTS ends
Previous ELTS Releases				
Debian 7 wheezy	i386, amd64	2013-05-04	2018-06-01	2020-06-30
Debian 8 jessie	i386, amd64, armhf, armel	2015-04-26	2020-07-01	2025-06-30
Current ELTS Release(s)				
Debian 9 stretch	i386, amd64, armhf	2017-06-17	2022-07-01	2027-06-30
Debian 10 buster	i386, amd64, armhf, arm64	2019-06-06	2024-07-01	2029-06-30
Future ELTS Release(s)				
Debian 11 bullseye	i386, amd64, ...?	2021-08-14	2026-09-01	2031-06-30
Debian 12 bookworm	i386, amd64, ...?	2023-06-10	2028-07-01	2033-06-30

ⓘ **Legend:**	End of life	**Supported by ELTS**	Future ELTS Version - Currently with LTS or Debian Oldstable support	Debian Stable support

CVE Analysis

- Investigation
  - Does it affect the version we distribute?
  - Does if affect the architecture we support?
  - Is it mitigated by a build flag?
- 40274 CVEs published in 2024
- Constant analysis work
  - security-tracker git repo
- Analysis available in the security-tracker
  - security-tracker.debian.org/
  - Shows affected versions
  - Shows fixed versions
  - ELTS: deb.freexian.com/extended-lts/tracker/
- Embargo - Confidential CVEs with a future publishing date

https://security-tracker.debian.org/tracker/source-package/curl (part 1)



Information on source package curl

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

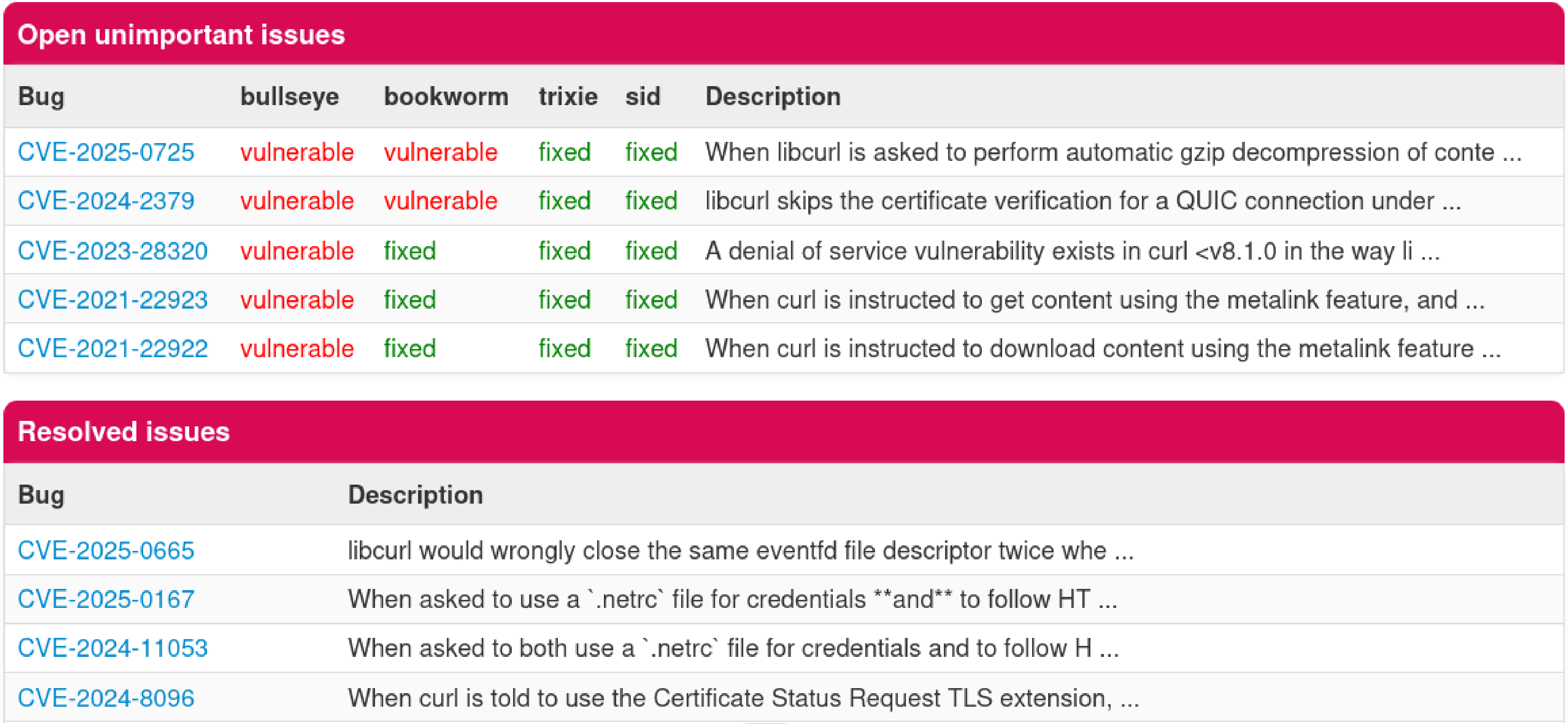
Available versions

Release	Version
bullseye	7.74.0-1.3+deb11u13
bullseye (security)	7.74.0-1.3+deb11u14
bookworm	7.88.1-10+deb12u12
bookworm (security)	7.88.1-10+deb12u5
trixie	8.13.0-1
sid	8.13.0-5

Open issues

Bug	bullseye	bookworm	trixie	sid	Description
CVE-2024-9681	vulnerable (no DSA, ignored)	fixed	fixed	fixed	When curl is asked to use HSTS, the expiry time for a subdomain might ...
CVE-2023-46219	vulnerable (no DSA, ignored)	fixed	fixed	fixed	When saving HSTS data to an excessively long file name, curl could end ...
CVE-2023-23915	vulnerable (no DSA, ignored)	fixed	fixed	fixed	A cleartext transmission of sensitive information vulnerability exists ...
CVE-2023-23914	vulnerable (no DSA, ignored)	fixed	fixed	fixed	A cleartext transmission of sensitive information vulnerability exists ...
CVE-2022-43551	vulnerable (no DSA, ignored)	fixed	fixed	fixed	A vulnerability exists in curl <7.87.0 HSTS check that could be bypass ...
CVE-2022-42916	vulnerable (no DSA, ignored)	fixed	fixed	fixed	In curl before 7.86.0, the HSTS check could be bypassed to trick it in ...

https://security-tracker.debian.org/tracker/source-package/curl (part 2)



Open unimportant issues

Bug	bullseye	bookworm	trixie	sid	Description
CVE-2025-0725	vulnerable	vulnerable	fixed	fixed	When libcurl is asked to perform automatic gzip decompression of conte ...
CVE-2024-2379	vulnerable	vulnerable	fixed	fixed	libcurl skips the certificate verification for a QUIC connection under ...
CVE-2023-28320	vulnerable	fixed	fixed	fixed	A denial of service vulnerability exists in curl <v8.1.0 in the way li ...
CVE-2021-22923	vulnerable	fixed	fixed	fixed	When curl is instructed to get content using the metalink feature, and ...
CVE-2021-22922	vulnerable	fixed	fixed	fixed	When curl is instructed to download content using the metalink feature ...

Resolved issues

Bug	Description
CVE-2025-0665	libcurl would wrongly close the same eventfd file descriptor twice whe ...
CVE-2025-0167	When asked to use a `.netrc` file for credentials **and** to follow HT ...
CVE-2024-11053	When asked to both use a `.netrc` file for credentials and to follow H ...
CVE-2024-8096	When curl is told to use the Certificate Status Request TLS extension, ...

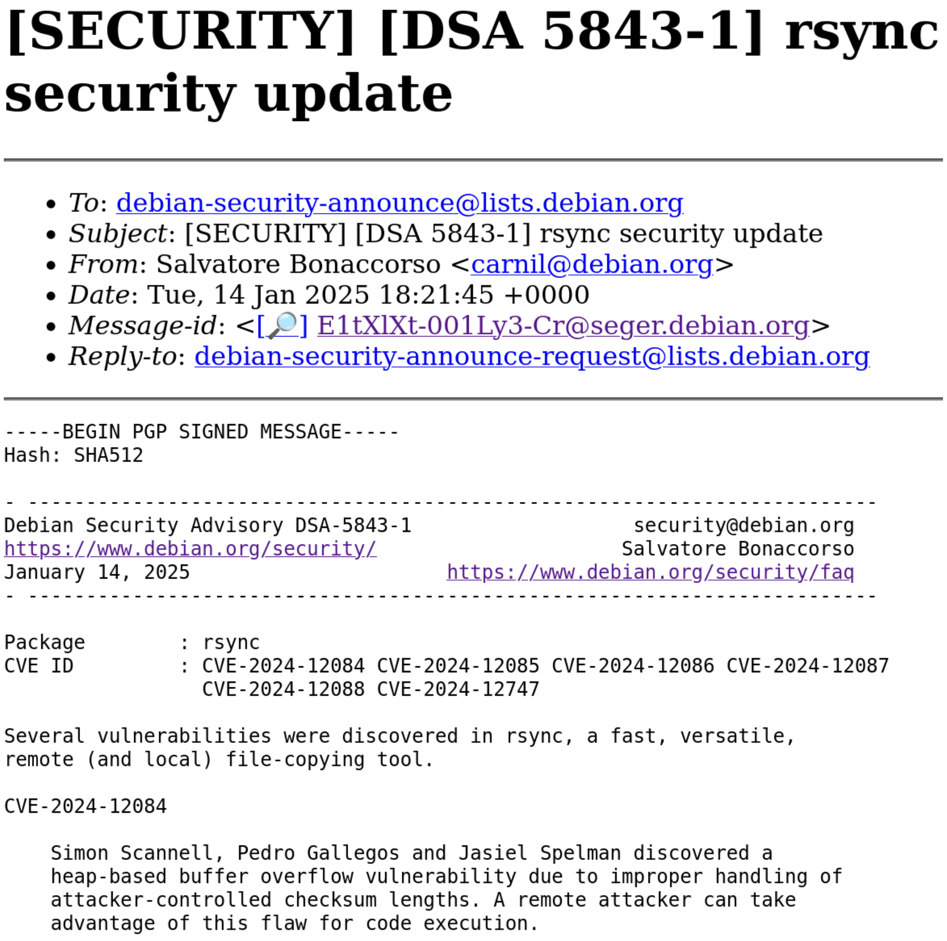
Upstream Fixes vs. Debian Fixes

- Upstream pushes a fix in version 5.0
- Debian ships versions 3.0 in Debian OldStable and 4.0 in Debian Stable
- Updating to 5.0 is out of scope for Debian Stable
  - Update to 5.0 requires configuration changes and user’s validation/testing
- Debian backports the fix from version 5.0 to the previous versions
  - Fixed version with backported patch
    - 4.0-2+deb12u1
    - 3.0-2+deb11u1

Advisories

- Debian Security Advisory – DSA
- Debian LTS Security Advisory – DLA
- Debian ELTS Security Advisory – ELA
- Where is the fix shipped
  - DSA, DLA, ELA: security repository
  - No advisory: proposed-updates and point-releases (ex.: Debian 12.7)
- www.debian.org/security/

DSA 5843-1 (part 1)

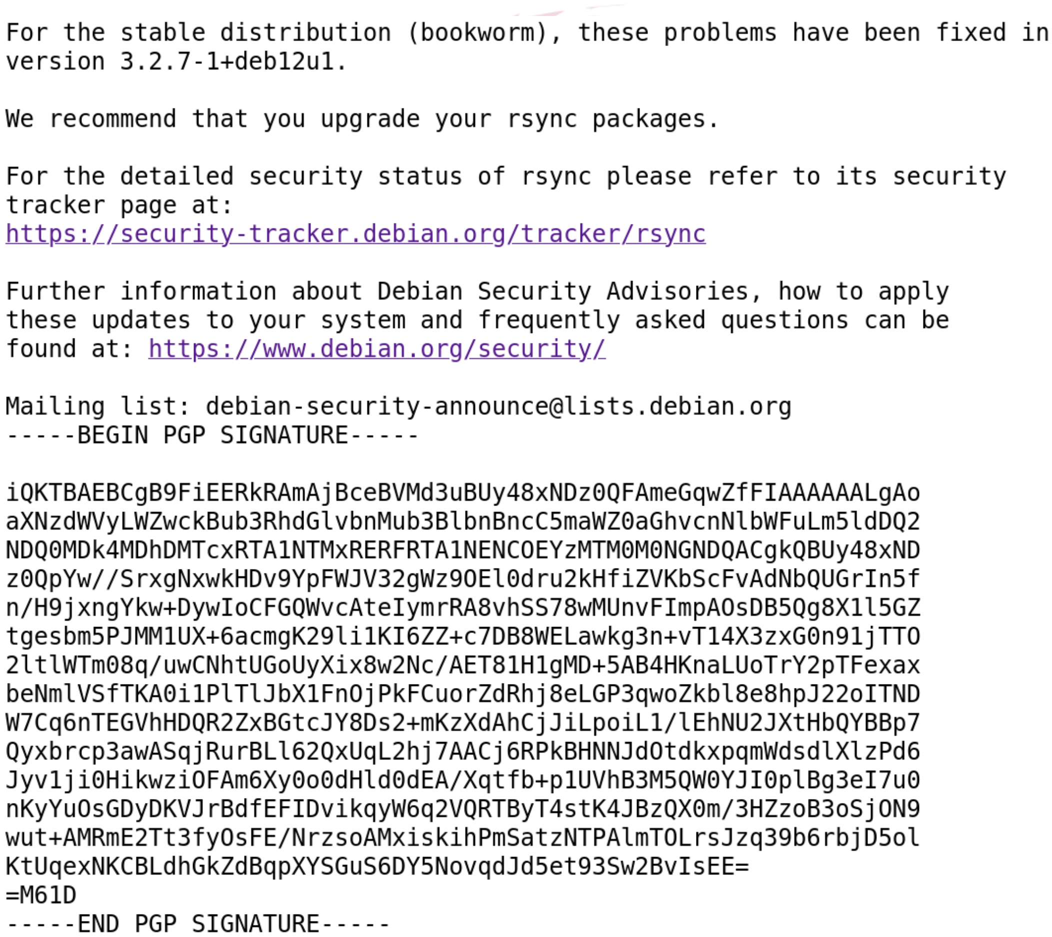


[SECURITY] [DSA 5843-1] rsync security update

- *To*: debian-security-announce@lists.debian.org
- *Subject*: [SECURITY] [DSA 5843-1] rsync security update
- *From*: Salvatore Bonaccorso <carnil@debian.org>
- *Date*: Tue, 14 Jan 2025 18:21:45 +0000
- *Message-id*: <[🔎] E1tXlXt-001Ly3-Cr@seger.debian.org>
- *Reply-to*: debian-security-announce-request@lists.debian.org

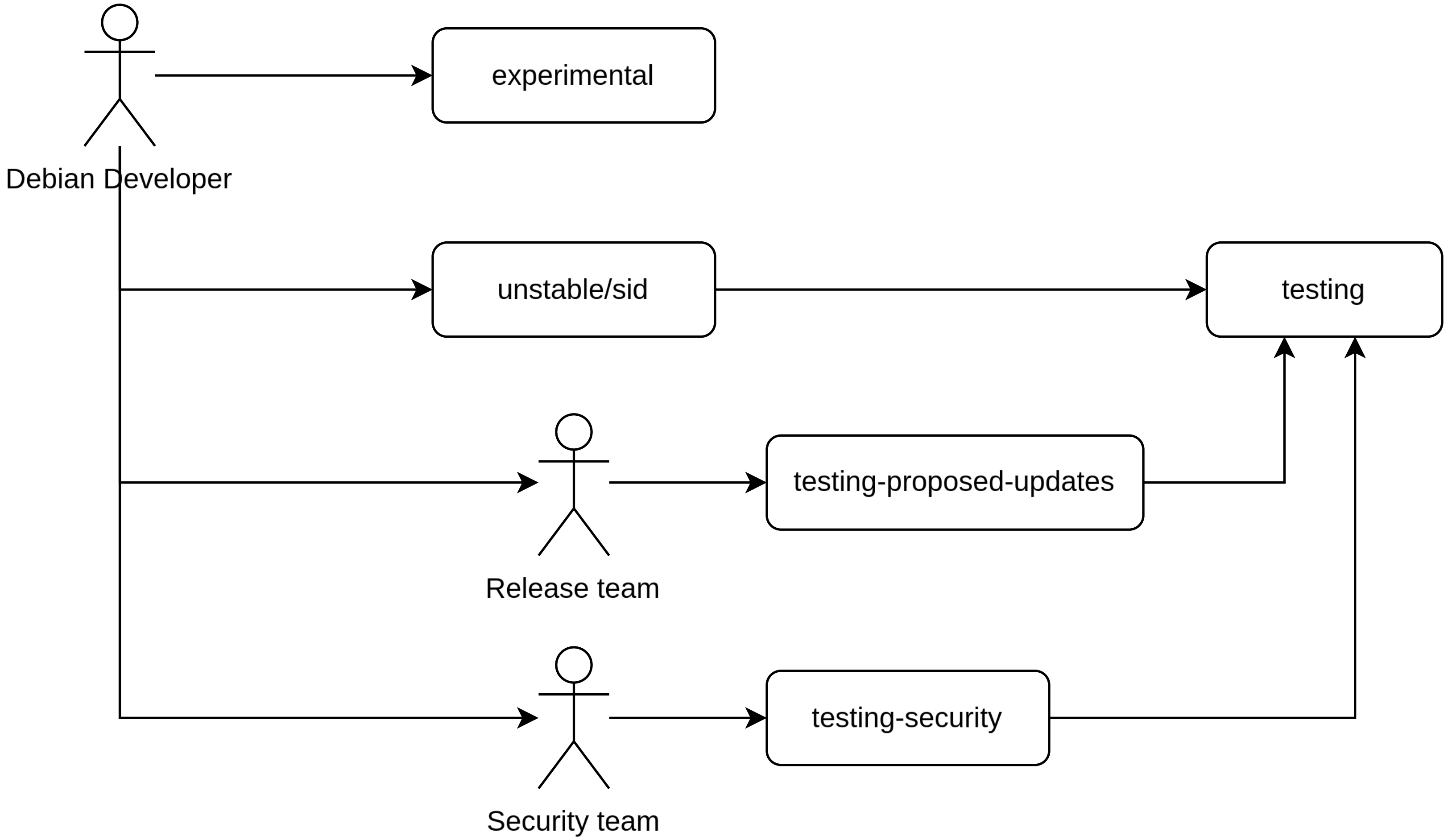
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

- -------------------------------------------------------------------------
Debian Security Advisory DSA-5843-1                   security@debian.org
https://www.debian.org/security/                     Salvatore Bonaccorso
January 14, 2025                      https://www.debian.org/security/faq
- -------------------------------------------------------------------------

Package        : rsync
CVE ID         : CVE-2024-12084 CVE-2024-12085 CVE-2024-12086 CVE-2024-12087
                 CVE-2024-12088 CVE-2024-12747

Several vulnerabilities were discovered in rsync, a fast, versatile,
remote (and local) file-copying tool.

CVE-2024-12084

    Simon Scannell, Pedro Gallegos and Jasiel Spelman discovered a
    heap-based buffer overflow vulnerability due to improper handling of
    attacker-controlled checksum lengths. A remote attacker can take
    advantage of this flaw for code execution.
```

DSA 5843-1 (part 2)

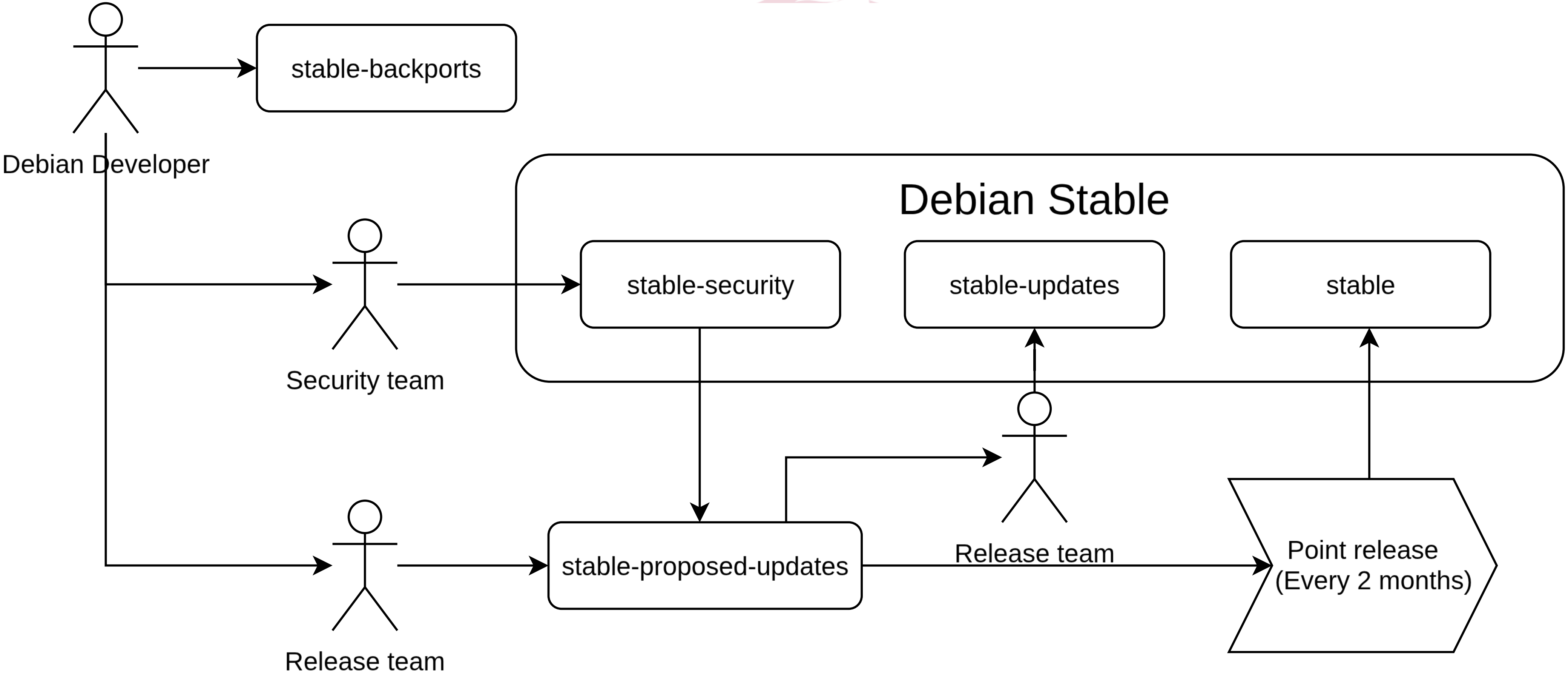


```
For the stable distribution (bookworm), these problems have been fixed in
version 3.2.7-1+deb12u1.

We recommend that you upgrade your rsync packages.

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

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-----

iQKTBAEBCgB9FiEERkRAmAjBceBVMd3uBUy48xNDz0QFAmeGqwZfFIAAAAAALgAo
aXNzdWVyLWZwckBub3RhdGlvbnMub3BlbnBncC5maWZ0aGhvcnNlbWFuLm5ldDQ2
NDQ0MDk4MDhDMTcxRTA1NTMxRERFRTA1NENCOEYzMTM0M0NGNDQACgkQBUy48xND
z0QpYw//SrxgNxwkHDv9YpFWJV32gWz9OEl0dru2kHfiZVKbScFvAdNbQUGrIn5f
n/H9jxngYkw+DywIoCFGQWvcAteIymrRA8vhSS78wMUnvFImpAOsDB5Qg8X1l5GZ
tgesbm5PJMM1UX+6acmgK29li1KI6ZZ+c7DB8WELawkg3n+vT14X3zxG0n91jTTO
2ltlWTm08q/uwCNhtUGoUyXix8w2Nc/AET81H1gMD+5AB4HKnaLUoTrY2pTFexax
beNmlVSfTKA0i1PlTlJbX1FnOjPkFCuorZdRhj8eLGP3qwoZkbl8e8hpJ22oITND
W7Cq6nTEGVhHDQR2ZxBGtcJY8Ds2+mKzXdAhCjJiLpoiL1/lEhNU2JXtHbQYBBp7
Qyxbrcp3awASqjRurBLl62QxUqL2hj7AACj6RPkBHNNJdOtdkxpqmWdsdlXlzPd6
Jyv1ji0HikwziOFAm6Xy0o0dHld0dEA/Xqtfb+p1UVhB3M5QW0YJI0plBg3eI7u0
nKyYuOsGDyDKVJrBdfEFIDvikqyW6q2VQRTByT4stK4JBzQX0m/3HZzoB3oSjON9
wut+AMRmE2Tt3fyOsFE/NrzsoAMxiskihPmSatzNTPAlmTOLrsJzq39b6rbjD5ol
KtUqexNKCBLdhGkZdBqpXYSGuS6DY5NovqdJd5et93Sw2BvIsEE=
=M61D
-----END PGP SIGNATURE-----
```

Debian Experimental, Unstable and Testing



Debian Stable and OldStable



Debian Developer

stable-backports

Debian Stable

stable-security

stable-updates

stable

Security team

Release team

stable-proposed-updates

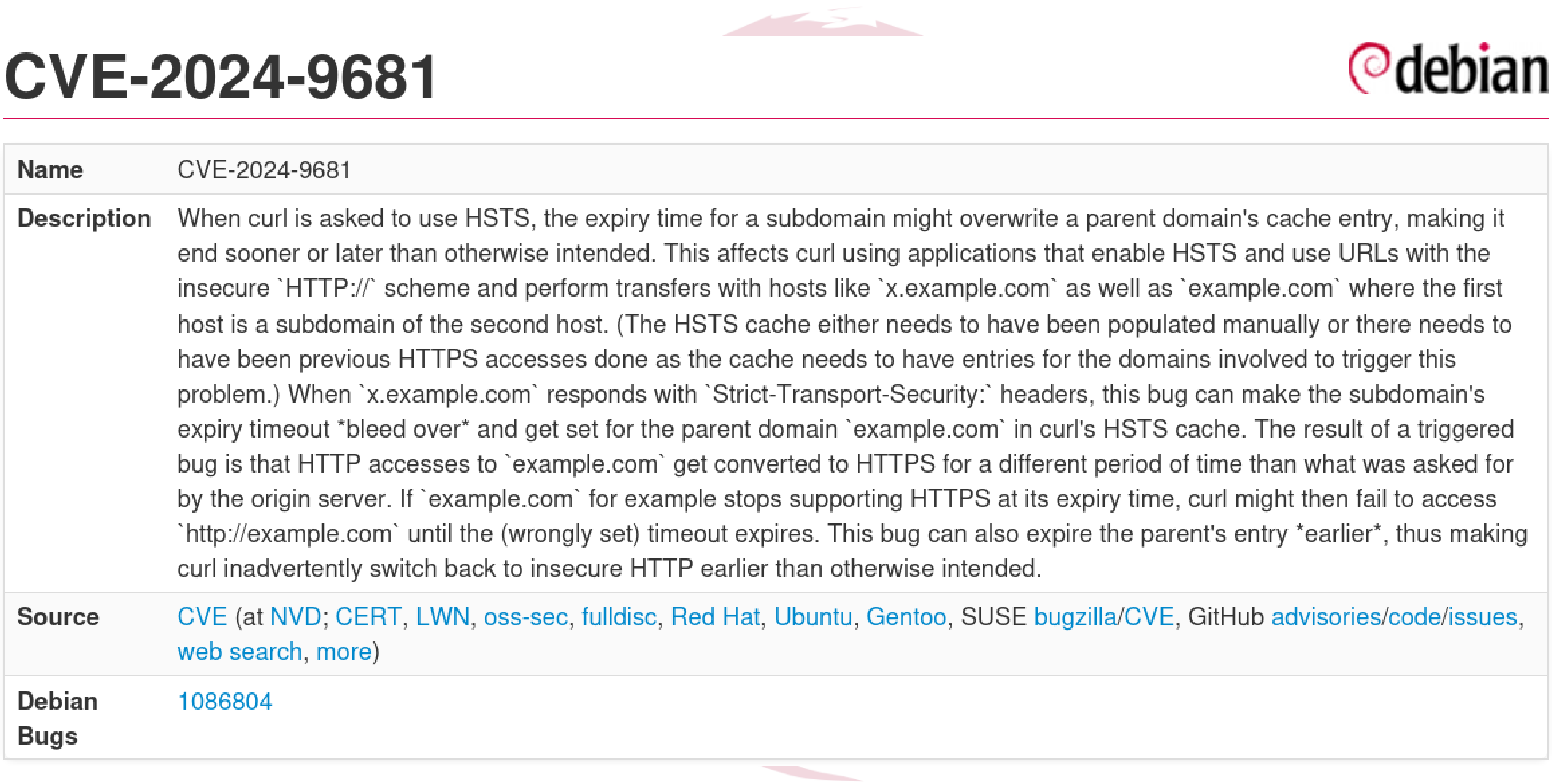
Release team

Point release (Every 2 months)

Reasons to not fix a CVE

- Risk Analysis
- Prioritization - Anybody can contribute
- Not a real security vulnerability
- Examples
  - Minimal impact, e.g.: crash
  - Fix is too complex and risks introducing other problems
  - Fix is removing a feature
- Vulnerabilities that are in the source code but not in the resulting binary

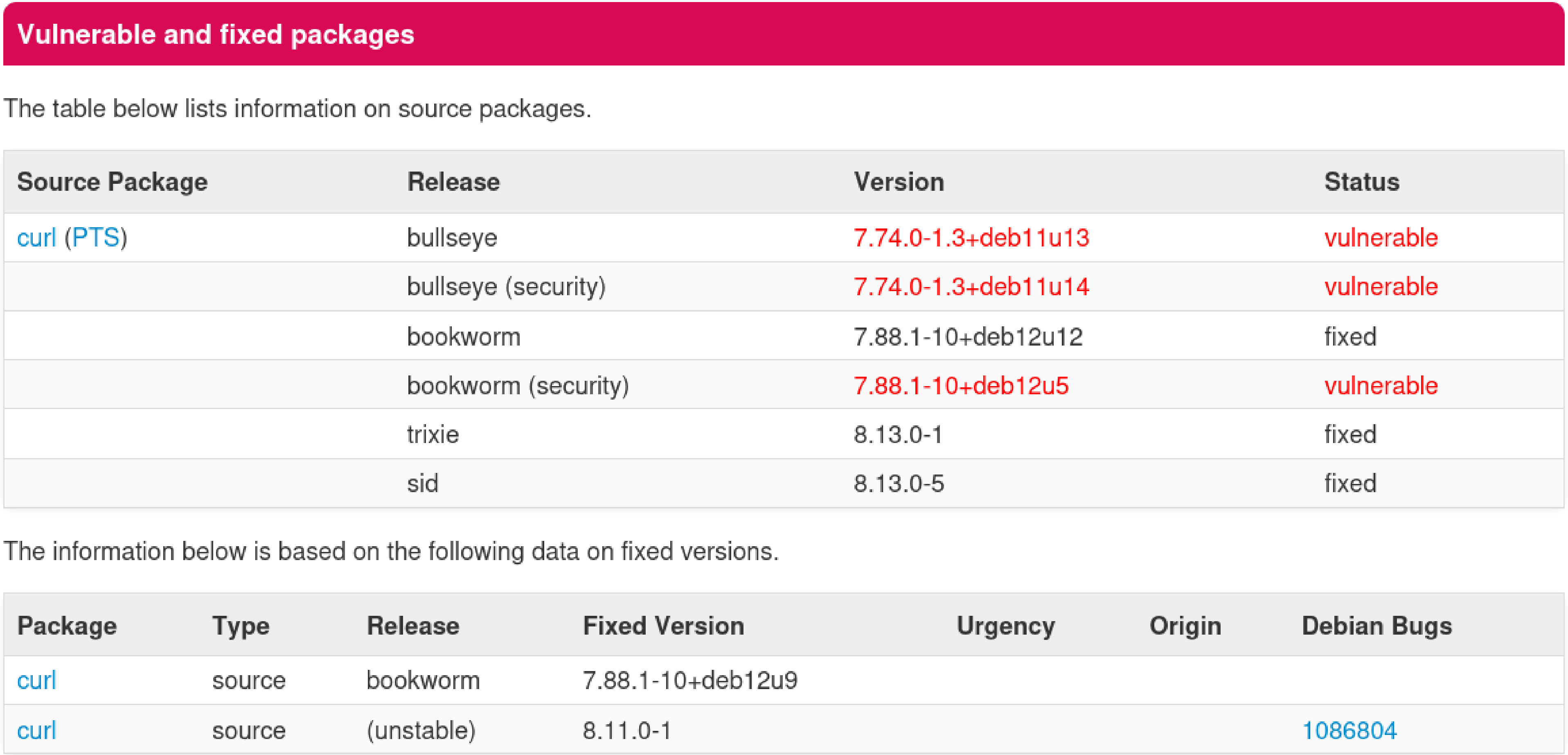
https://security-tracker.debian.org/tracker/CVE-2024-9681 (part 1)



CVE-2024-9681

Name	CVE-2024-9681
Description	When curl is asked to use HSTS, the expiry time for a subdomain might overwrite a parent domain's cache entry, making it end sooner or later than otherwise intended. This affects curl using applications that enable HSTS and use URLs with the insecure \`HTTP://\` scheme and perform transfers with hosts like \`x.example.com\` as well as \`example.com\` where the first host is a subdomain of the second host. (The HSTS cache either needs to have been populated manually or there needs to have been previous HTTPS accesses done as the cache needs to have entries for the domains involved to trigger this problem.) When \`x.example.com\` responds with \`Strict-Transport-Security:\` headers, this bug can make the subdomain's expiry timeout *bleed over* and get set for the parent domain \`example.com\` in curl's HSTS cache. The result of a triggered bug is that HTTP accesses to \`example.com\` get converted to HTTPS for a different period of time than what was asked for by the origin server. If \`example.com\` for example stops supporting HTTPS at its expiry time, curl might then fail to access \`http://example.com\` until the (wrongly set) timeout expires. This bug can also expire the parent's entry *earlier*, thus making curl inadvertently switch back to insecure HTTP earlier than otherwise intended.
Source	CVE (at NVD; CERT, LWN, oss-sec, fulldisc, Red Hat, Ubuntu, Gentoo, SUSE bugzilla/CVE, GitHub advisories/code/issues, web search, more)
Debian Bugs	1086804

https://security-tracker.debian.org/tracker/CVE-2024-9681 (part 2)



Vulnerable and fixed packages

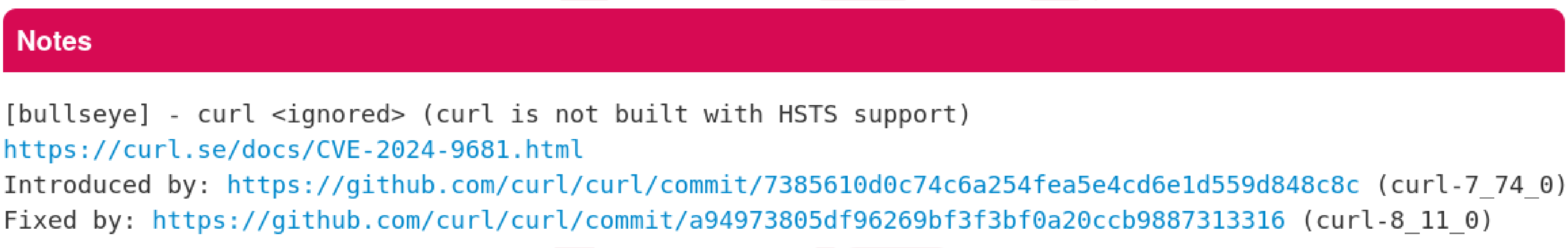
The table below lists information on source packages.

Source Package	Release	Version	Status
curl (PTS)	bullseye	7.74.0-1.3+deb11u13	vulnerable
	bullseye (security)	7.74.0-1.3+deb11u14	vulnerable
	bookworm	7.88.1-10+deb12u12	fixed
	bookworm (security)	7.88.1-10+deb12u5	vulnerable
	trixie	8.13.0-1	fixed
	sid	8.13.0-5	fixed

The information below is based on the following data on fixed versions.

Package	Type	Release	Fixed Version	Urgency	Origin	Debian Bugs
curl	source	bookworm	7.88.1-10+deb12u9			
curl	source	(unstable)	8.11.0-1			1086804

https://security-tracker.debian.org/tracker/CVE-2024-9681 (part 3)



Notes

```
[bullseye] - curl <ignored> (curl is not built with HSTS support)
https://curl.se/docs/CVE-2024-9681.html
Introduced by: https://github.com/curl/curl/commit/7385610d0c74c6a254fea5e4cd6e1d559d848c8c (curl-7_74_0)
Fixed by: https://github.com/curl/curl/commit/a94973805df96269bf3f3bf0a20ccb9887313316 (curl-8_11_0)
```

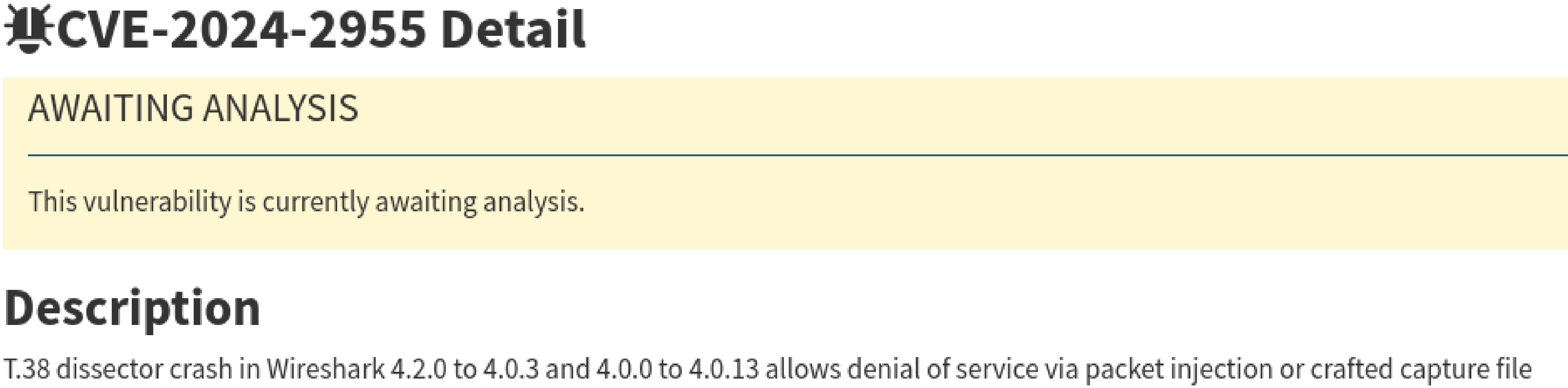
Signal-to-Noise ratio (in 2024)

- 40274 CVEs released
- 255 DSAs for Stable
  - 2046 CVEs fixed - **5%**
- 307 DLAs for OldStable
  - 2838 CVEs fixed - **7%**
- 149 CVEs added to CISA’s Known Exploited Vulnerabilities Catalog (KEV) – **~0.4%**
  - 93 without relationship to Debian (e.g.: Windows), leaving 56 CVEs left - **~0.01%**
  - **CVEs outside of KEV are NOT noise, but this ratio is an important indicator**
- 40274 CVEs -> 2046 DSA CVEs -> 56 relevant KEV
- github.com/samueloph/generate_cve_stats_debian_2024

Investigate It Yourself

- Start with the Security Tracker
- nvd.nist.gov for extra references
- Serious CVEs
  - Rapidly notified in tech news
  - Tend to have its own name, and even a logo
  - Were likely part of an embargo and Debian was involved
- Consider mitigating factors
- Be critical of the CVE description

https://nvd.nist.gov/vuln/detail/CVE-2024-2955



CVE-2024-2955 Detail

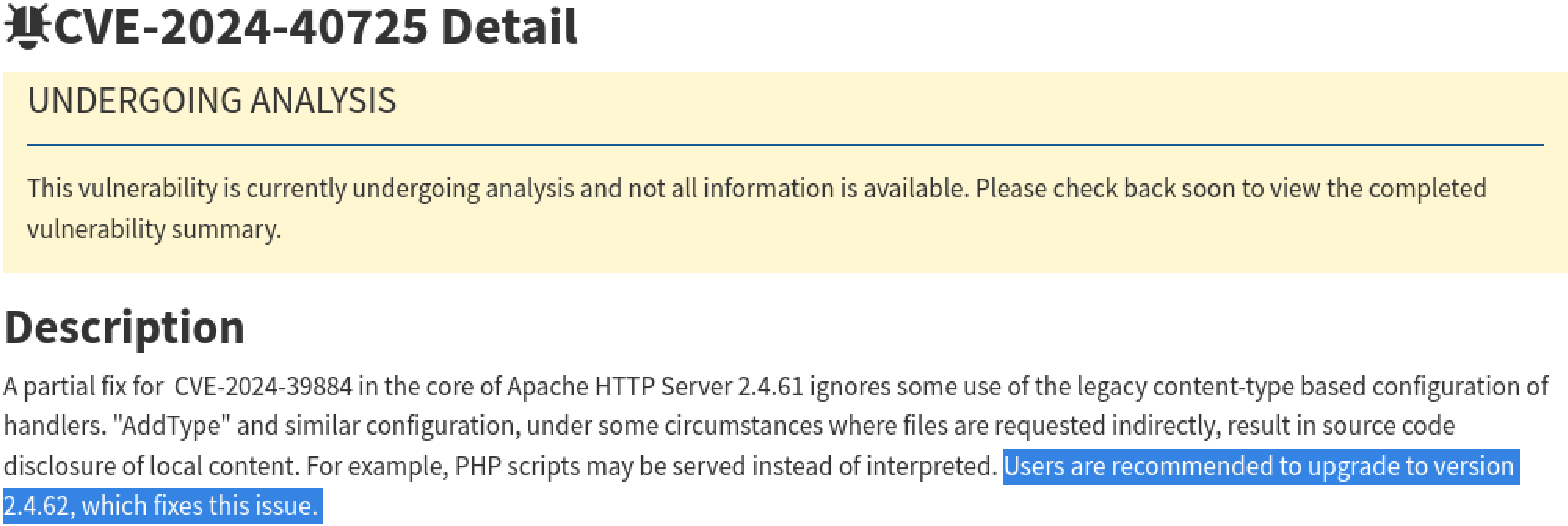
AWAITING ANALYSIS

This vulnerability is currently awaiting analysis.

Description

T.38 dissector crash in Wireshark 4.2.0 to 4.0.3 and 4.0.0 to 4.0.13 allows denial of service via packet injection or crafted capture file

https://nvd.nist.gov/vuln/detail/CVE-2024-40725



CVE-2024-40725 Detail

UNDERGOING ANALYSIS

This vulnerability is currently undergoing analysis and not all information is available. Please check back soon to view the completed vulnerability summary.

Description

A partial fix for CVE-2024-39884 in the core of Apache HTTP Server 2.4.61 ignores some use of the legacy content-type based configuration of handlers. "AddType" and similar configuration, under some circumstances where files are requested indirectly, result in source code disclosure of local content. For example, PHP scripts may be served instead of interpreted. Users are recommended to upgrade to version 2.4.62, which fixes this issue.

Good Practices

- Know your distributions’s security development practices
- Update frequently
- Reboot (if needed)
- Take extra care with unofficial packages
- Unused packages and services increase your risk exposure

tl;dr: "too long; didn't read"

- Security Tracker is the canonical source for vulnerability information:
  - security-tracker.debian.org/tracker/
- Affected package != Affected system
- A lot of CVEs are just noise
- Important fixes have an advisory and come through the security repository
- Be wary of derivative distributions

Questions?

- I’ll be here during the whole conference, feel free to reach out.

Muito obrigado!

The Security of Debian

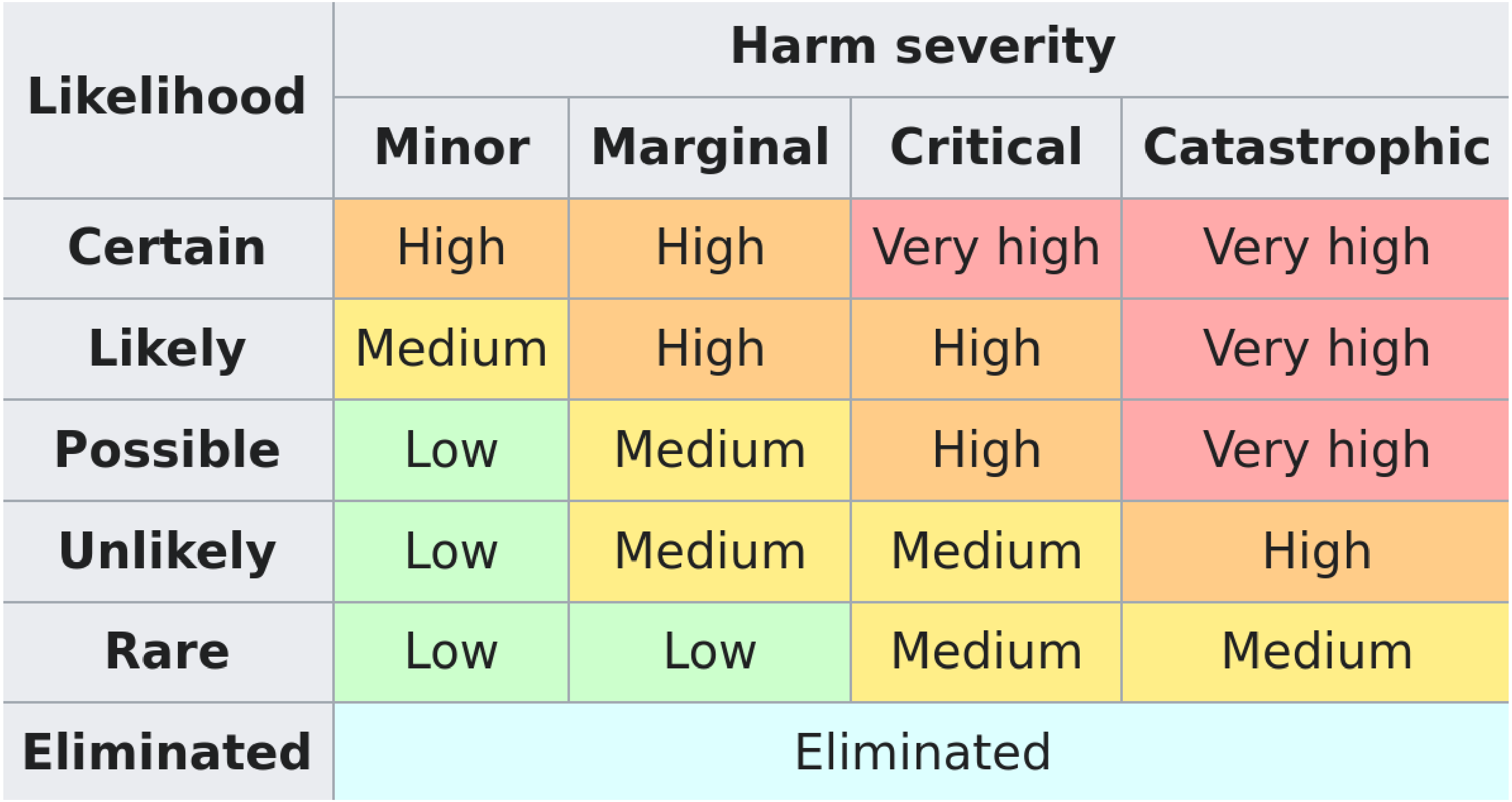
An Introduction for Advanced Users

DebConf 25

Brest, France

Slides avialable at samueloph.dev/slides

https://en.wikipedia.org/wiki/Risk_matrix



Likelihood	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			