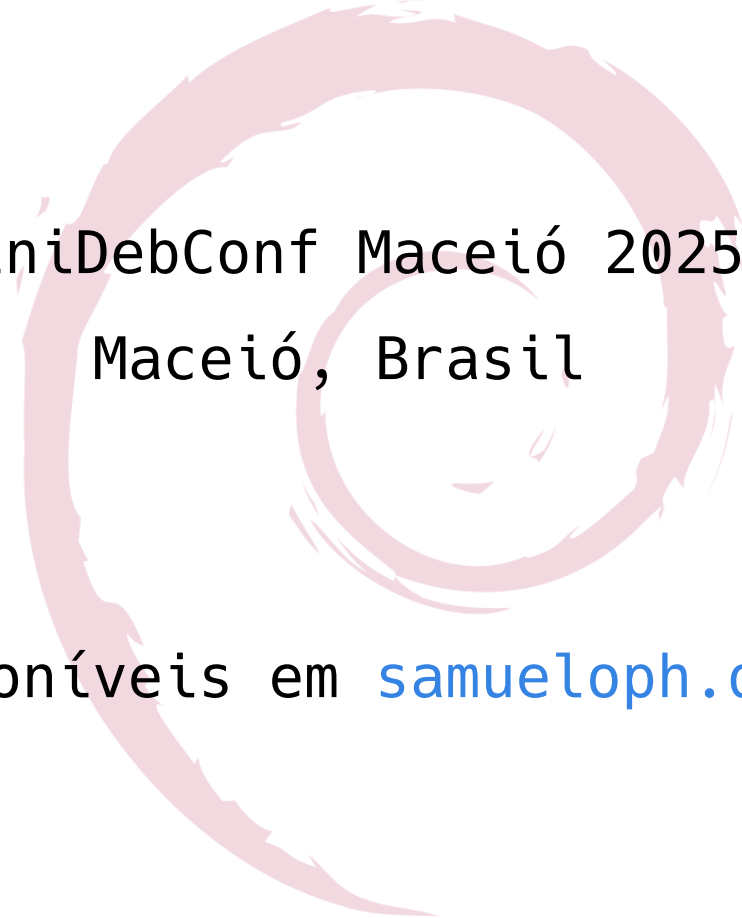


A Segurança do Debian




MiniDebConf Maceió 2025
Maceió, Brasil

Slides disponíveis em samueloph.dev/slides

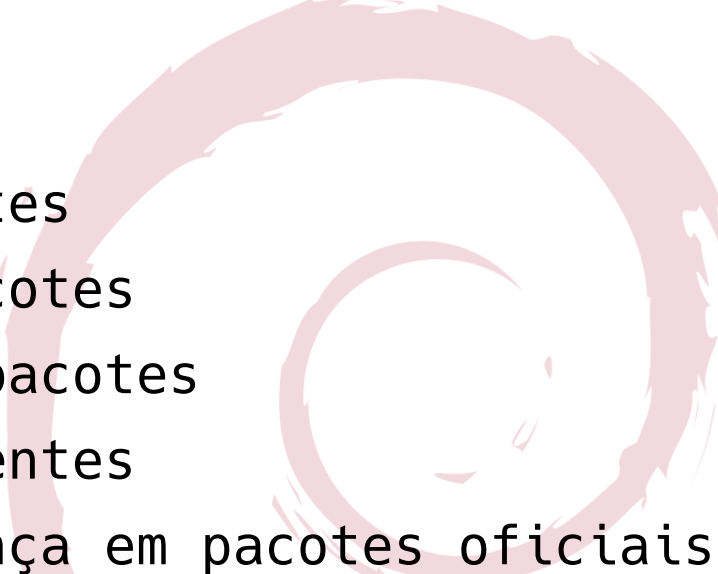
Sobre mim

- Samuel Henrique <samueloph>
- *Debian Developer* desde 2018
 - Voluntário, não remunerado
- Membro do *Security Tools Packaging Team*
- Mantém curl, rsync, shellcheck...
- Mentoria de iniciantes para empacotamento
- *Senior System Development Engineer* no Amazon Linux, time de segurança
- Debian/Linux, Python, Rust, Bash, Security
- linkedin.com/in/samueloph
- samueloph.dev

Sumário

- CVEs
 - Suporte Debian
 - Análise de CVEs
 - Correção de CVEs
 - Distribuição de correções
 - Investigando você mesmo
 - Equívocos comuns
 - Boas práticas
- 

Aspectos da segurança

- Infra-estrutura
 - Governança
 - Ingestão de pacotes
 - Construção de pacotes
 - Distribuição de pacotes
 - Resposta a incidentes
 - Falhas de segurança em pacotes oficiais
- 

Common Vulnerabilities and Exposures (CVE)


- Criado em 1999 pelo MITRE, bancado pelo governo estadunidense
 - cve.org
- Coordenação de anúncio de problemas de segurança com banco de dados público
- Qualquer pessoa pode reportar/requerir um CVE-ID
 - cve.org/ReportRequest/ReportRequestForNonCNAs
- ID universal
 - CVE-YYYY-NNNN, ex.: CVE-2023-4911
 - cve.org/CVERecord?id=CVE-2023-4911.
- Outras organizações enriquecem os dados de uma CVE, via republicação:
 - NIST/NVD - Score e severidade
 - 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/2023/2023_top25_list.html

Alternativas a CVE


- Alternativas:
 - Github - GHSA: github.com/advisories/GHSA-m77w-6vjw-wh2f
 - *Distributed Weakness Filing (DWF)* - Inativo
 - RustSec Advisory Database: rustsec.org
 - Go Vulnerability Database - GO-YYYY-NNNN: pkg.go.dev/vuln
 - Entidades geopolíticas
 - Japão
 - China
 - Rússia
 - Europa - CERT-EU


Suporte Debian

- 3 anos pelo time de segurança
- +2 anos pelo time de LTS
- +5 anos pelo time de ELTS
 - Suporte provido pela empresa Freexian
 - Necessário uso de repositório externo
 - Financiado por clientes Freexian, porém disponível gratuitamente para todos
- 10 anos ao total



Version	support architecture	schedule
Debian 7 "Wheezy"	i386, amd64	from 2018-06-01 to 2020-06-30
Debian 8 "Jessie"	i386, amd64, armhf, armel	from 2020-07-01 to 2025-06-30
Debian 9 "Stretch"	i386, amd64, armhf	from 2022-07-01 to 2027-06-30
Debian 10 "Buster"	i386, amd64, armhf, arm64	from 2024-07-01 to 2029-06-30
Debian 11 "Bullseye"	i386, amd64, ...?	from 2026-09-01 to 2031-06-30
Debian 12 "Bookworm"	i386, amd64, ...?	from 2028-07-01 to 2033-06-30



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

Análise de CVEs

- Investigação
 - Afeta a versão que distribuímos?
 - Afeta a arquitetura que distribuímos?
 - É mitigada por alguma *build flag*?
 - É mitigada por alguma *feature* desabilitada?
- 40009 CVEs publicadas em 2024
- Trabalho constante do time de segurança
 - [repositório do security-tracker](#)
- Análises disponíveis no security-tracker
 - security-tracker.debian.org/
 - ELTS: deb.freexian.com/extended-lts/tracker/
 - Lista versões afetadas
 - Lista correções
- Embargo - CVEs privadas com data de publicação

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> (parte 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, ...

Correções Upstream vs. Correções Debian

- Upstream corrige na versão 5.0
- Debian disponibiliza versões 3.0 e 4.0 no Debian Stable e Debian Oldstable
- Atualizar para 5.0 está fora do escopo do Debian stable
 - Atualizar a partir das versões 3.0/4.0 para 5.0 requer mudanças de configurações e validação de usuários
- Debian faz o “*backport*” da correção da versão 5.0 para as versões anteriores
 - Exemplo de versão corrigida: 4.0-2+deb12u2

Advisories

- Debian Security Advisory - DSA
- Debian LTS Security Advisory - DLA
- Debian ELTS Security Advisory - ELA
- Repositório a ser usado
 - DSA, DLA, ELA: Repositório security
 - Sem advisory: *Proposed-updates* e *point-releases* (ex.: *Debian 12.7*)
- www.debian.org/security/

DSA 5843-1 (parte 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: <E1tXIXt-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 (parte 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/>

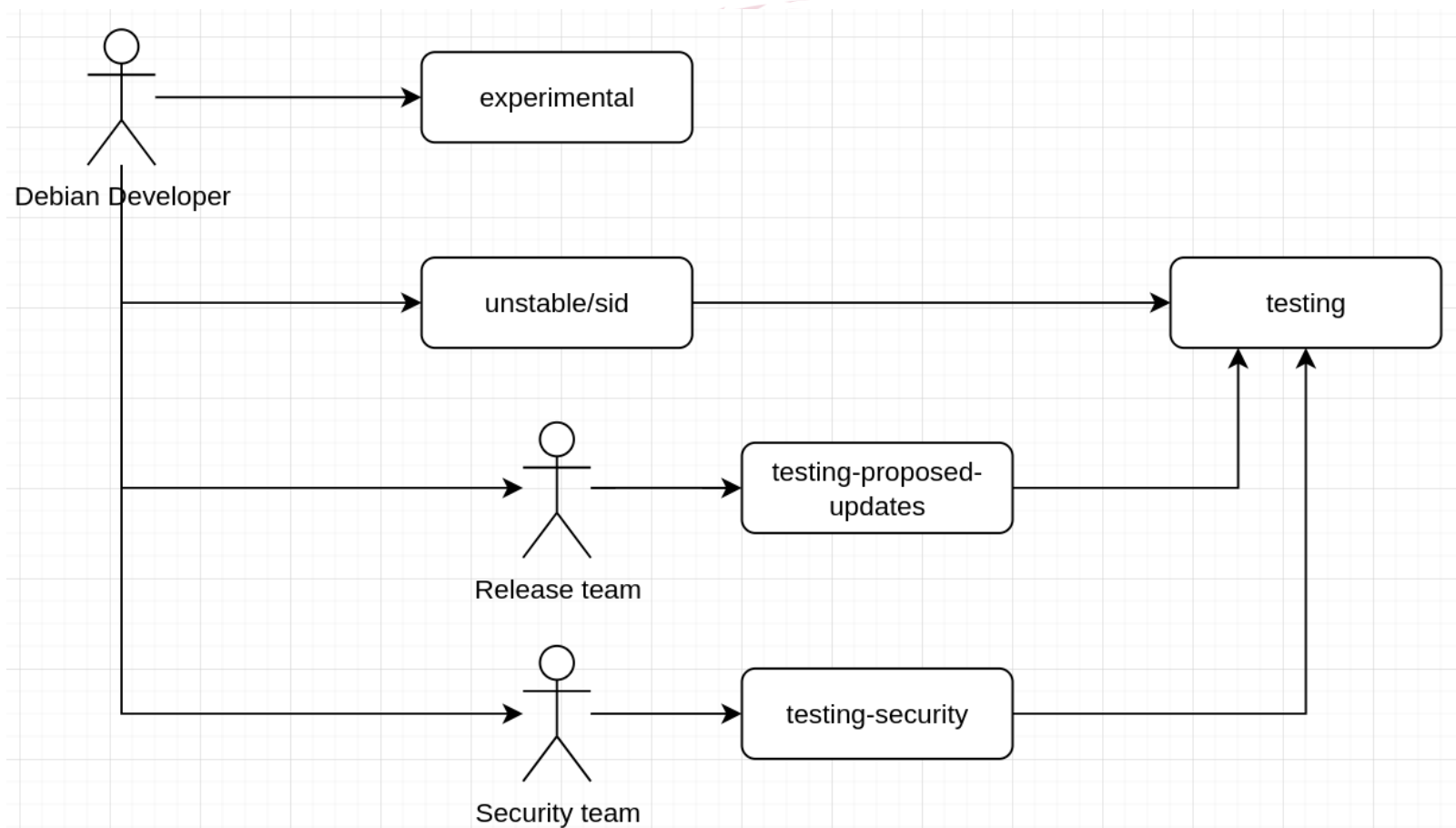
Mailing list: debian-security-announce@lists.debian.org

-----BEGIN PGP SIGNATURE-----

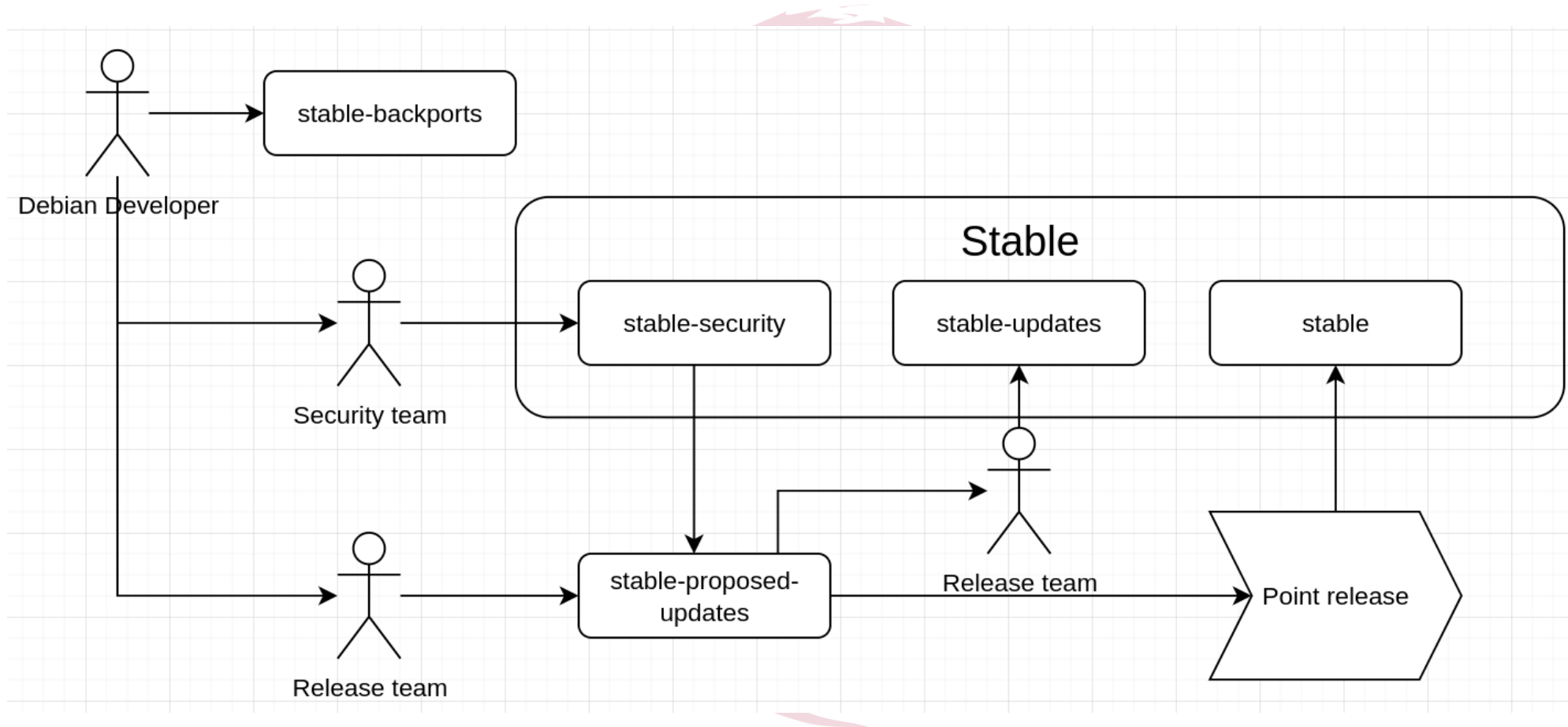
```
iQKTBAEBCgB9FiEERkRAmAjBceBVMd3uBUy48xNDz0QFAmeGqwZfFIAAAAAALgAo
aXNzdWVyLWZwckBub3RhdGlbnMub3BlbnBncC5maWZ0aGhvcnNlbWFuLm5ldDQ2
NDQ0MDk4MDhDMTcxRTA1NTMxRERFRTA1NENC0EYzMTM0M0NGNDQACgkQBUIy48xND
z0QpYw//SrxgNxwKHdV9YpFWJV32gWz90El0dru2kHfiZVKbScFvAdNbQUGrIn5f
n/H9jxngYkw+DyWIoCFGQWvcAteIymrRA8vhSS78wMUnvFImpA0sDB5Qg8X1l5GZ
tgesbm5PJMM1UX+6acmgK29li1KI6ZZ+c7DB8WELawkg3n+vT14X3zxG0n91jTT0
2ltlWTm08q/uwCNhtUGoUyXix8w2Nc/AET81HlgMD+5AB4HKnaLUoTrY2pTFexax
beNmlVSfTKA0i1PlTLJbX1Fn0jPkFCuorZdRhj8eLGP3qwoZkbl8e8hpJ22oITND
W7Cq6nTEGVhHDQR2ZxBGtcJY8Ds2+mKzXdAhCjJiLpoiL1/lEhNU2JXtHbQYBBp7
Qyxbrcp3awASqjRurBLl62QxUqL2hj7AACj6RPkBHNNJd0tdkxpmWdsdLXlzPd6
Jyv1ji0Hikwzi0Fam6Xy0o0dHld0dEA/Xqtfb+p1UVhB3M5QW0YJI0plBg3eI7u0
nKyYu0sGDyDKVJRbdfEFIDvikqyW6q2VQRTByT4stK4JBzQX0m/3HZzoB3oSj0N9
wut+AMRmE2Tt3fy0sFE/NrzsoAMxiskihPmSatzNTPAlmTOLrsJzq39b6rbjD5oL
KtUqexNKCBLdhGkZdBqpXYSGuS6DY5NovqdJd5et93Sw2BvIsEE=
=M61D
```

-----END PGP SIGNATURE-----

Debian Experimental, Unstable e Testing



Debian Stable e OldStable



Motivos para não corrigir CVEs

- Análise de risco
- Priorização - voluntários bem-vindos
- Não é uma falha de segurança real
- Exemplos
 - Impacto mínimo - *crash*
 - Correção é muito complexa e introduz riscos
 - Remoção de feature como correção
- Vulnerabilidade está apenas no código-fonte, não no pacote final

CVE-2024-9681



Name	CVE-2024-9681
Description	<p>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 <code>`HTTP://`</code> scheme and perform transfers with hosts like <code>`x.example.com`</code> as well as <code>`example.com`</code> 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 <code>`x.example.com`</code> responds with <code>`Strict-Transport-Security:`</code> headers, this bug can make the subdomain's expiry timeout <i>*bleed over*</i> and get set for the parent domain <code>`example.com`</code> in curl's HSTS cache. The result of a triggered bug is that HTTP accesses to <code>`example.com`</code> get converted to HTTPS for a different period of time than what was asked for by the origin server. If <code>`example.com`</code> for example stops supporting HTTPS at its expiry time, curl might then fail to access <code>`http://example.com`</code> until the (wrongly set) timeout expires. This bug can also expire the parent's entry <i>*earlier*</i>, thus making curl inadvertently switch back to insecure HTTP earlier than otherwise intended.</p>
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

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

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)

Muito barulho, pouco sinal

- Em 2024:
- 40009 CVEs lançadas no MITRE
- 7347 CVEs analisadas pelo Debian - **~18%**
- 255 DSAs para o Stable
- 307 DLAs para o OldStable
- 185 CVEs adicionadas no Catálogo de Vulnerabilidades Conhecidas Exploradas (CISA KEV) - **~0.5%**
 - 78 claramente não tem relação nenhuma com Debian (ex.: Windows), restando 107 - **~0.3%**
 - **Embora incorreto assumir que CVEs fora do KEV não são um risco, essa proporção é um indicador importante**

Investigando você mesmo

- Security-tracker como fonte principal
- nvd.nist.gov
- CVEs graves são noticiadas rapidamente nas mídias tech
- CVEs muito graves
 - Costumam ganhar nome próprio e logótipo
 - Provavelmente foram parte de um embargo e o Debian esteve envolvido
- Considere fatores mitigantes
- Seja crítico com relação a descrição da CVE



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





CVE-2024-40725 Detail

UNDERGOING ANALYSIS

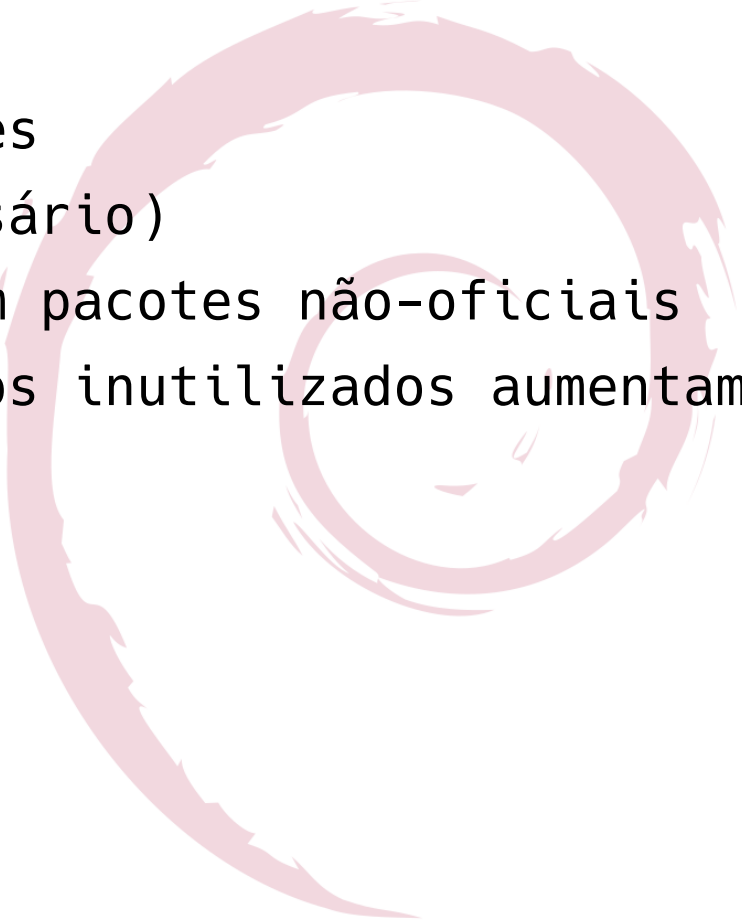
This vulnerability is currently undergoing analysis and not all information is available. Please check back soon to view the completed vulnerability summary.

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.](#)



Boas práticas

- USE DEBIAN!
 - Updates frequentes
 - Reboot (se necessário)
 - Cuidado extra com pacotes não-oficiais
 - Pacotes e serviços inutilizados aumentam riscos
- 

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

- Security Tracker é a fonte canônica de informações sobre CVEs e o Debian: security-tracker.debian.org/tracker/
- Pacote afetado != Sistema afetado
- Muitas CVEs são spam
- Correções importantes contém advisory e vem pelo repositório de segurança
- Cuidado com distribuições derivadas

Perguntas?

Estarei aqui durante toda a conferência, sintam-se livres para conversar comigo



Muito obrigado!

A segurança do Debian

MiniDebConf Maceió 2025

Maceió, Brasil

Slides disponíveis em samueloph.dev/slides

Probabilidade	Gravidade			
	Leve	Marginal	Crítico	Catastrófico
Certo	Alto	Alto	Muito alto	Muito alto
Provável	Médio	Alto	Alto	Muito alto
Possível	Baixo	Médio	Alto	Muito alto
Improvável	Baixo	Médio	Médio	Alto
Raro	Baixo	Baixo	Médio	Médio
Eliminado	Eliminado			