Fixing CVEs on Debian

Everything you probably know already

DebConf24

Busan, Korea

Slides available at samueloph.dev/slides

About me

- Samuel Henrique <samueloph>
- Debian Developer since 2018
- Member of the Security Tools Packaging Team
- Maintains curl, rsync, shellcheck...
- Mentorship for newcomers learning packaging
- System Development Engineer for Amazon Linux, security team
- Debian/Linux, Python, Rust, Bash, Security
- linkedin.com/in/samueloph
- samueloph.dev

Summary

- CVE introduction
- CVEs for Debian
- How upstream vs how Debian fix CVEs
- Steps to fix a CVE
  - Examples and things I wish I knew before starting

The CVE® Program and the CVE ID

- CVE ID: Global identifier for vulnerabilities
- Format: CVE-YYYY-NNNNN, for example: CVE-2024-3094
- Crowdsorced effort
- Unique per vulnerability
- Main source of vulnerability data worldwide
- Mutable
- Can contain misleading information
- cve.org

A CVE for Debian

- security-tracker.debian.org
- Debian constantly monitor CVE updates
- 80 new CVEs published daily on average for 2023
- Can be fixed by people that are not in the security team
- Might release advisories for fixes; DSA, DLA, BSA (Freexian's ELA)
- Fixed with “backporting”, not to be confused with the backports repository

How upstream developers fix CVEs

- CVE gets reported against version 5.0
- 1) Upstream pushes a fix bundled with other changes in version 6.0; OR
- 2) Upstream pushes a fix as release 5.1, does not say anything about version 4 because it’s not supported anymore; OR
- 3) Upstream is extremely nice and kind and points out the exact commits or versions that both introduced and fixed the CVE (even if they don’t support it anymore). AFAIK only curl is doing this today

How Debian fix CVEs

- Upstream provided a fix as a new release versioned 6.0
- Debian ships 5.0-1 (testing/unstable) and 4.0-1 (stable)
- For testing and unstable: package the latest release as 6.0-1
- For stable, oldstable and older: backport the fix into the package, example for stable: 4.0-1+deb12u1
- (optional) Release an advisory anouncing the update: Debian Security Advisory (DSA), DLA, ELA, BSA

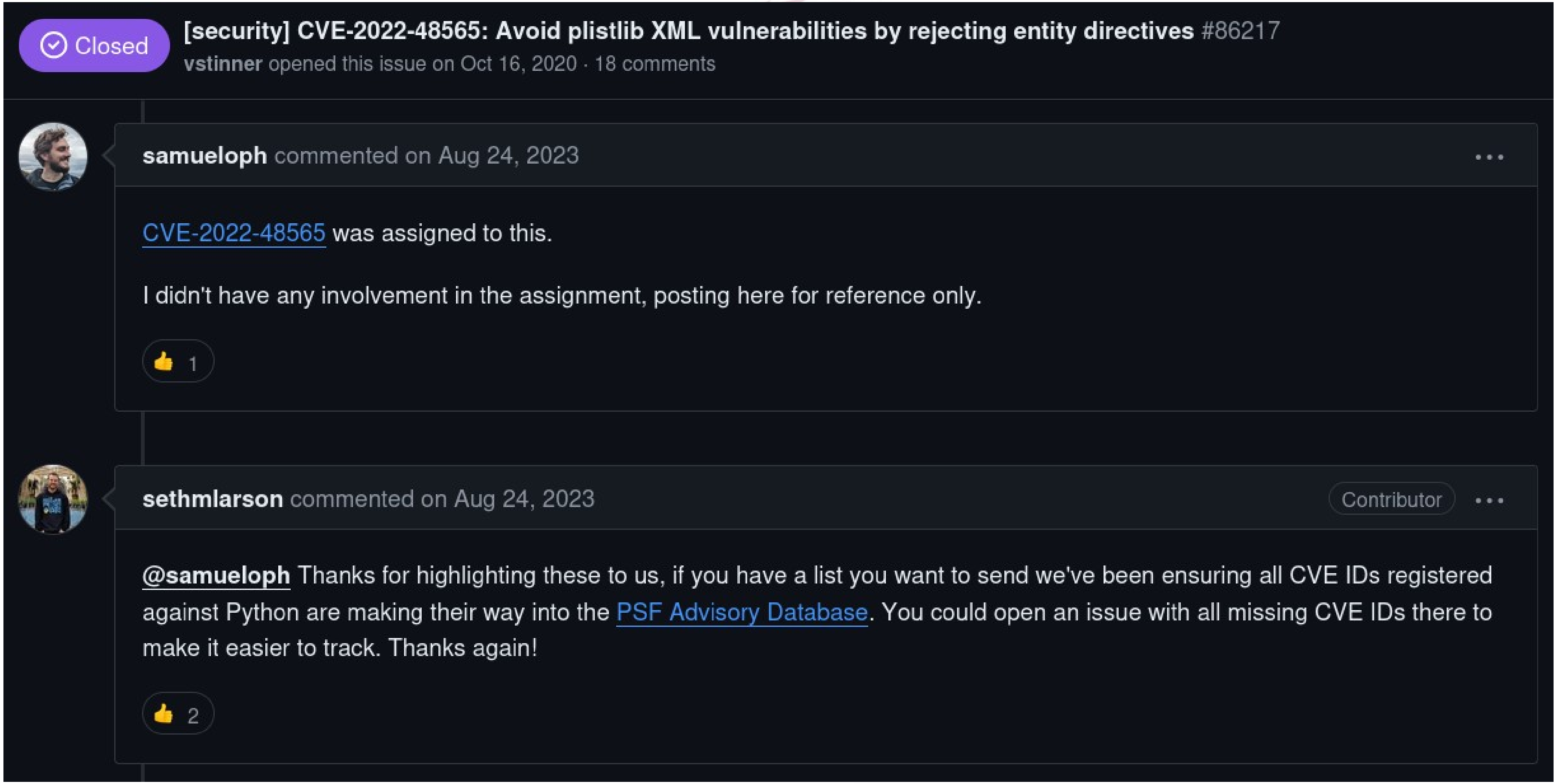
Steps to fix a CVE

- Find a CVE to fix
- Confirm impact
- Identify the fix
- Apply the patches to the Debian packaging
  - Modify the patch as needed, document it
  - Review backporting changes
- Test the changes
- Submit the fixed package
- Follow-up to check for reported regressions

Find a CVE to fix

- security-tracker.debian.org
  - Check CVE notes
- No-DSA for beginners - proposed-updates
- DSA requires security team coordination
  - Consider doing more than one fix for a single DSA
- Contact package maintainer (BTS)
- Is it acknowledged by the upstream developers?
- Not every CVE should be fixed

https://github.com/python/cpython/issues/86217#issuecomment-1691958323



Closed **[security] CVE-2022-48565: Avoid plistlib XML vulnerabilities by rejecting entity directives** #86217

vstinner opened this issue on Oct 16, 2020 · 18 comments

samueloph commented on Aug 24, 2023

CVE-2022-48565 was assigned to this.

I didn't have any involvement in the assignment, posting here for reference only.

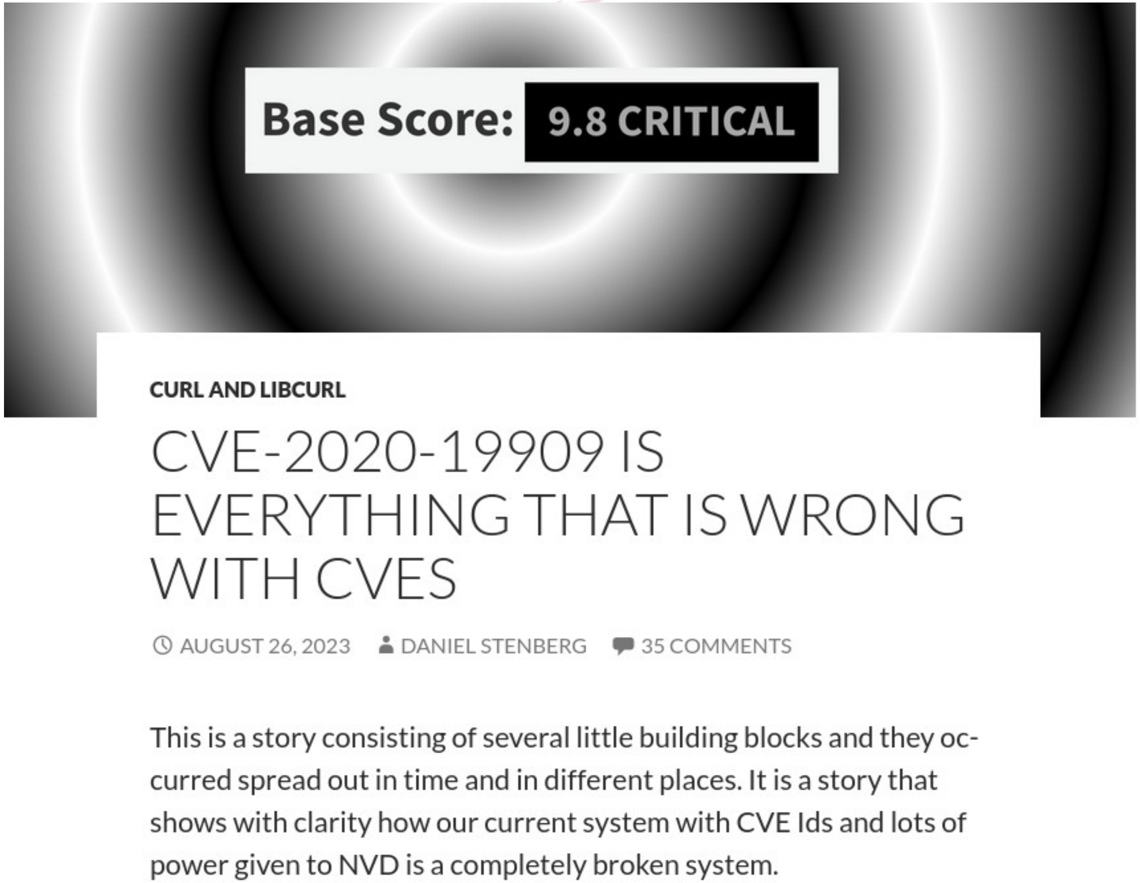
👍 1

sethmlarson commented on Aug 24, 2023 Contributor

@samueloph Thanks for highlighting these to us, if you have a list you want to send we've been ensuring all CVE IDs registered against Python are making their way into the PSF Advisory Database. You could open an issue with all missing CVE IDs there to make it easier to track. Thanks again!

👍 2

https://daniel.haxx.se/blog/2023/08/26/cve-2020-19909-is-everything-that-is-wrong-with-cves/



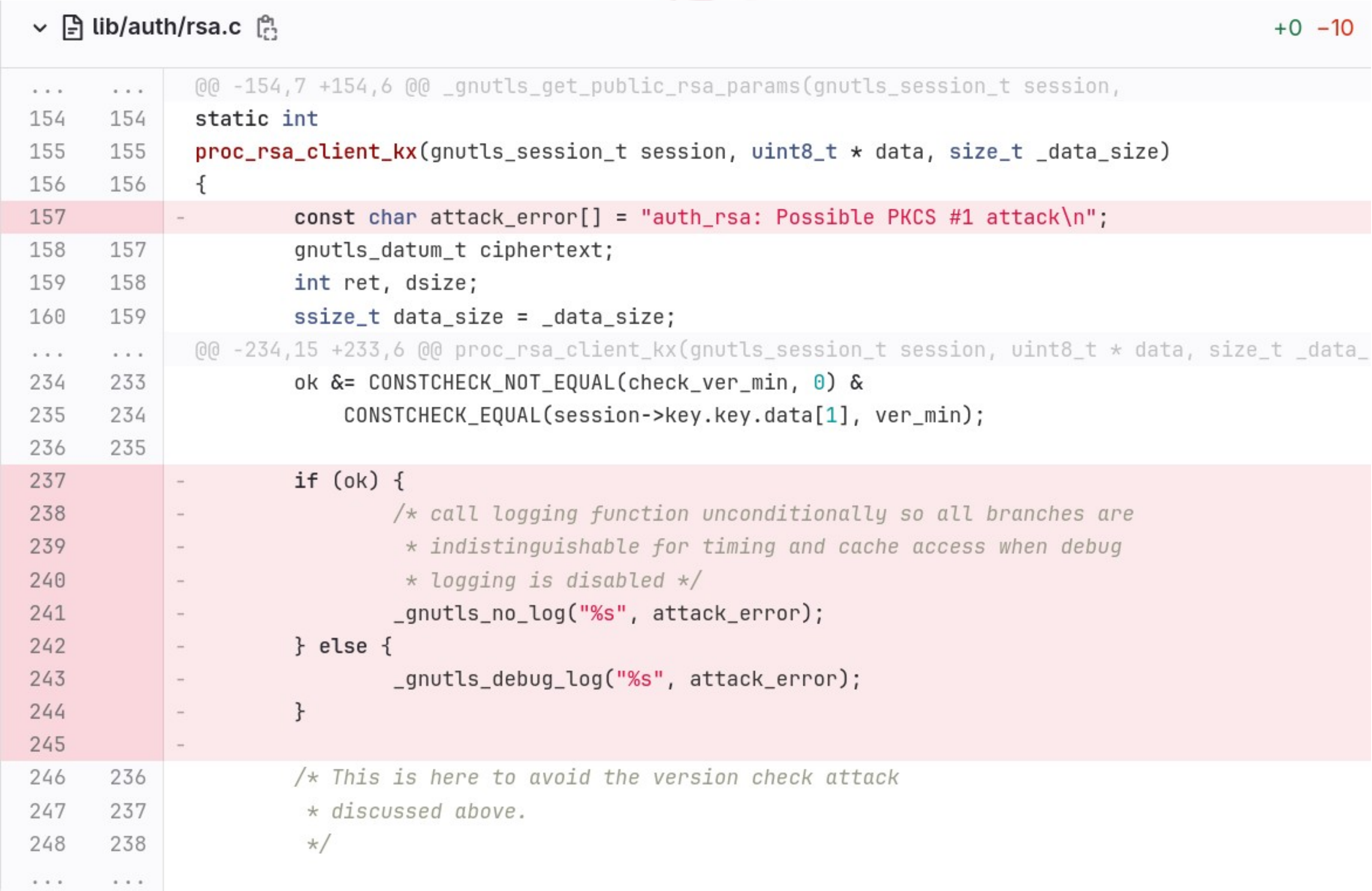
CURL AND LIBCURL

CVE-2020-19909 IS EVERYTHING THAT IS WRONG WITH CVES

AUGUST 26, 2023 DANIEL STENBERG 35 COMMENTS

This is a story consisting of several little building blocks and they occurred spread out in time and in different places. It is a story that shows with clarity how our current system with CVE Ids and lots of power given to NVD is a completely broken system.

https://gitlab.com/gnutls/gnutls/-/commit/80a6ce8ddb02477cd724cd5b2944791aaddb702a

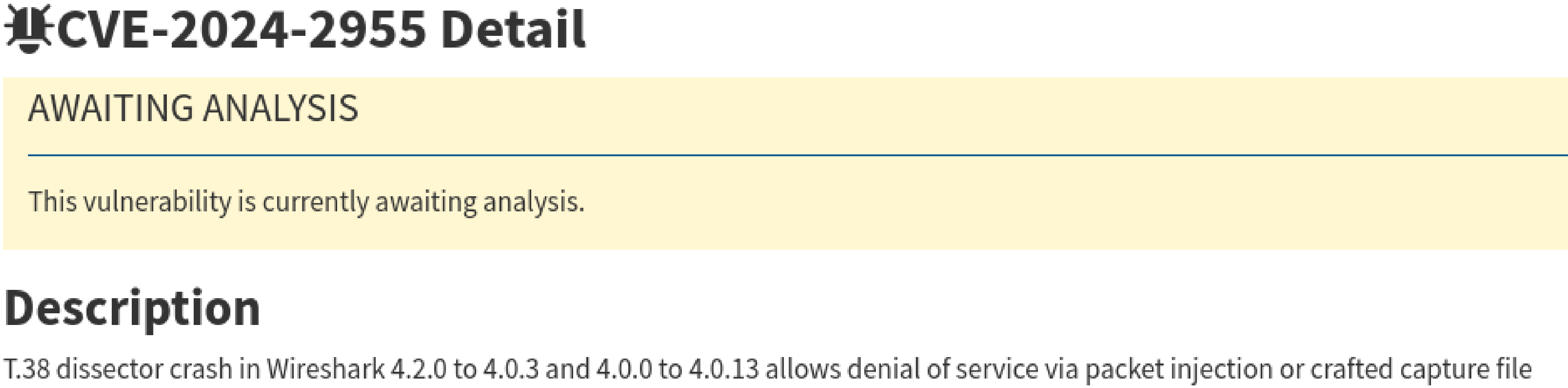


```diff
@@ -154,7 +154,6 @@ _gnutls_get_public_rsa_params(gnutls_session_t session,
 static int
 proc_rsa_client_kx(gnutls_session_t session, uint8_t * data, size_t _data_size)
 {
-        const char attack_error[] = "auth_rsa: Possible PKCS #1 attack\n";
         gnutls_datum_t ciphertext;
         int ret, dsize;
         ssize_t data_size = _data_size;
@@ -234,15 +233,6 @@ proc_rsa_client_kx(gnutls_session_t session, uint8_t * data, size_t _data_
         ok &= CONSTCHECK_NOT_EQUAL(check_ver_min, 0) &
             CONSTCHECK_EQUAL(session->key.key.data[1], ver_min);
 
-        if (ok) {
-                /* call logging function unconditionally so all branches are
-                 * indistinguishable for timing and cache access when debug
-                 * logging is disabled */
-                _gnutls_no_log("%s", attack_error);
-        } else {
-                _gnutls_debug_log("%s", attack_error);
-        }
-
         /* This is here to avoid the version check attack
          * discussed above.
          */
...
```

Confirm impact

- 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?
  - Our security-tracker says “affected” even if we don’t build the affected code in cases where the vulnerability is in the sources
- Does hardening blocks the exploitation?
- Could the vulnerability have been backported?
- Update security-tracker with findings
- Affected code bundled into another package?
  - codesearch.debian.net
- Which Debian releases are affected?
- Don’t trust the CVE description, verify

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



CVE-2024-2955 Detail

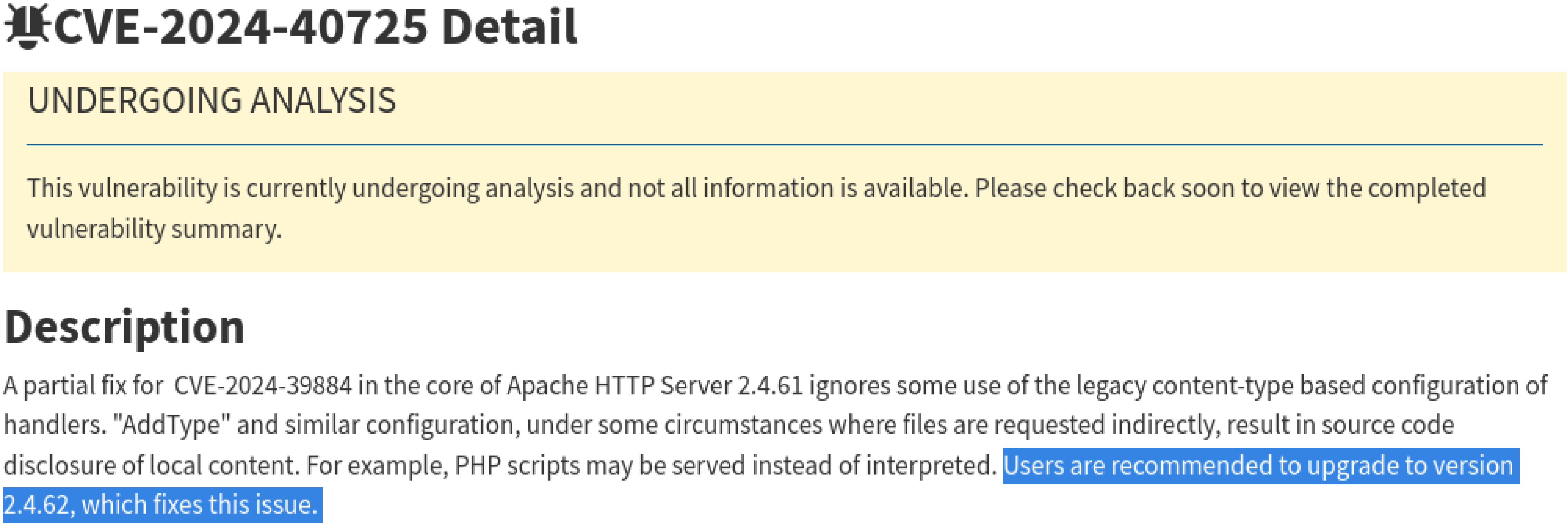
AWAITING ANALYSIS

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

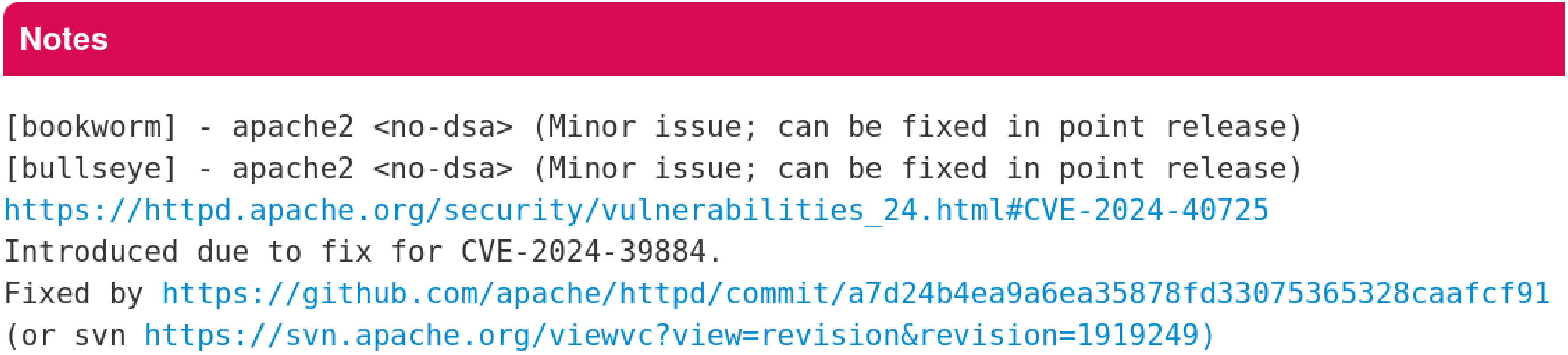
UNDERGOING ANALYSIS

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.

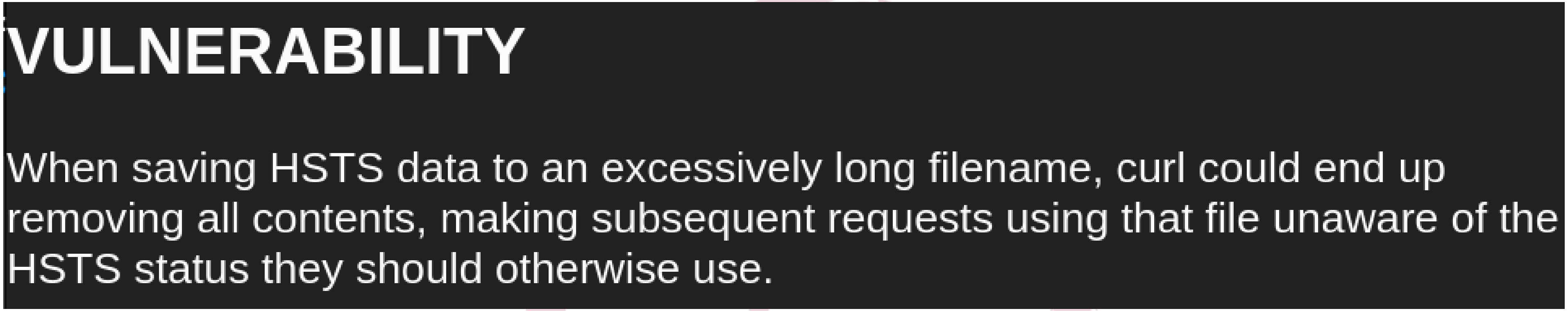
https://security-tracker.debian.org/tracker/CVE-2024-40725



Notes

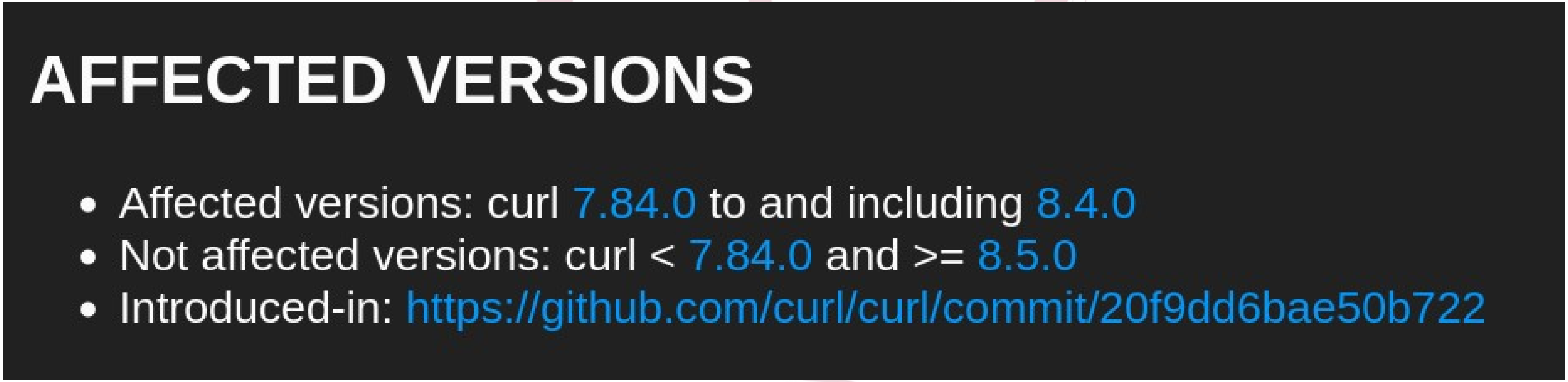
```
[bookworm] - apache2 <no-dsa> (Minor issue; can be fixed in point release)
[bullseye] - apache2 <no-dsa> (Minor issue; can be fixed in point release)
https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2024-40725
Introduced due to fix for CVE-2024-39884.
Fixed by https://github.com/apache/httpd/commit/a7d24b4ea9a6ea35878fd33075365328caafcf91
(or svn https://svn.apache.org/viewvc?view=revision&revision=1919249)
```

https://curl.se/docs/CVE-2023-46219.html



VULNERABILITY

When saving HSTS data to an excessively long filename, curl could end up removing all contents, making subsequent requests using that file unaware of the HSTS status they should otherwise use.



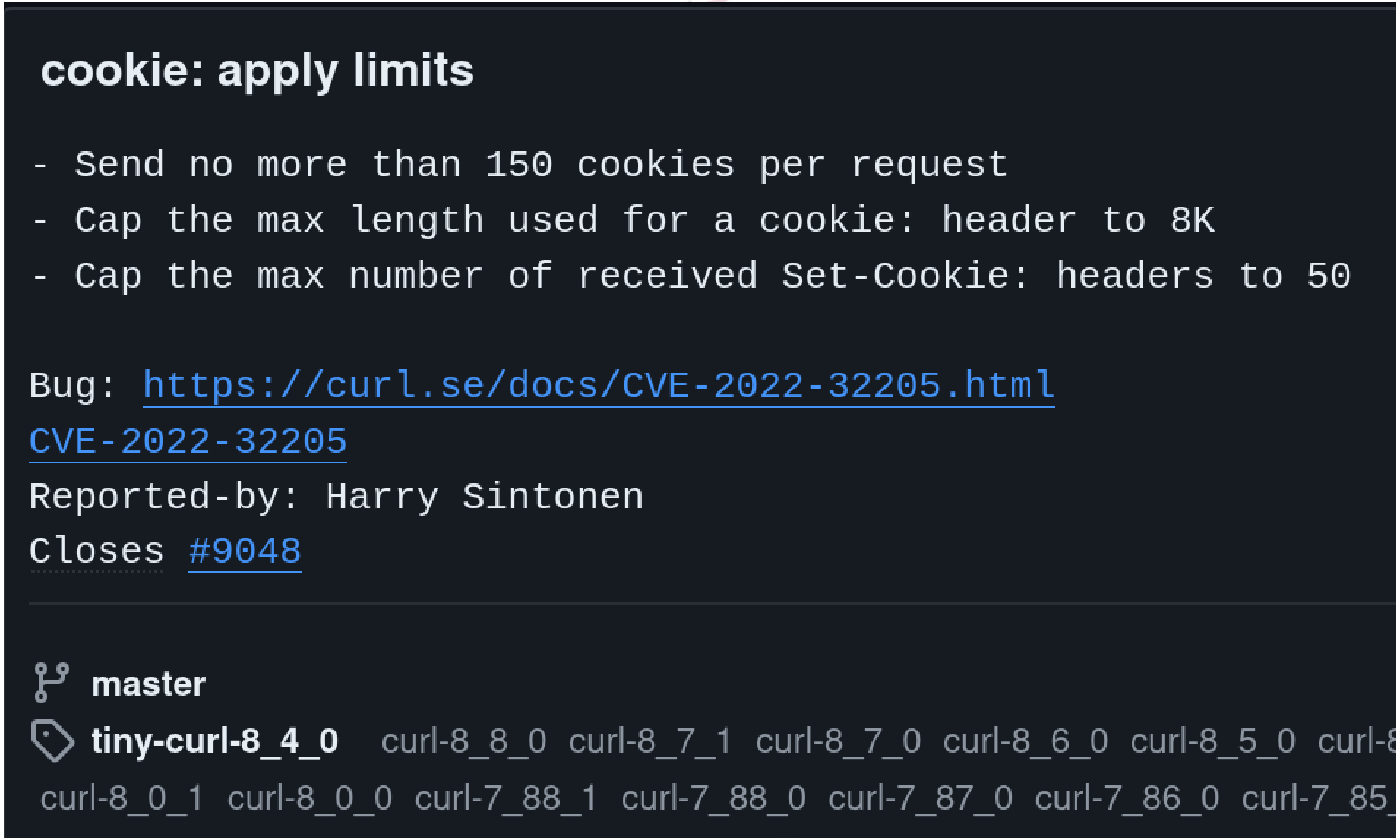
AFFECTED VERSIONS

- Affected versions: curl 7.84.0 to and including 8.4.0
- Not affected versions: curl < 7.84.0 and >= 8.5.0
- Introduced-in: https://github.com/curl/curl/commit/20f9dd6bae50b722

Identify the fix

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

https://github.com/curl/curl/commit/48d7064a49148f0394



cookie: apply limits

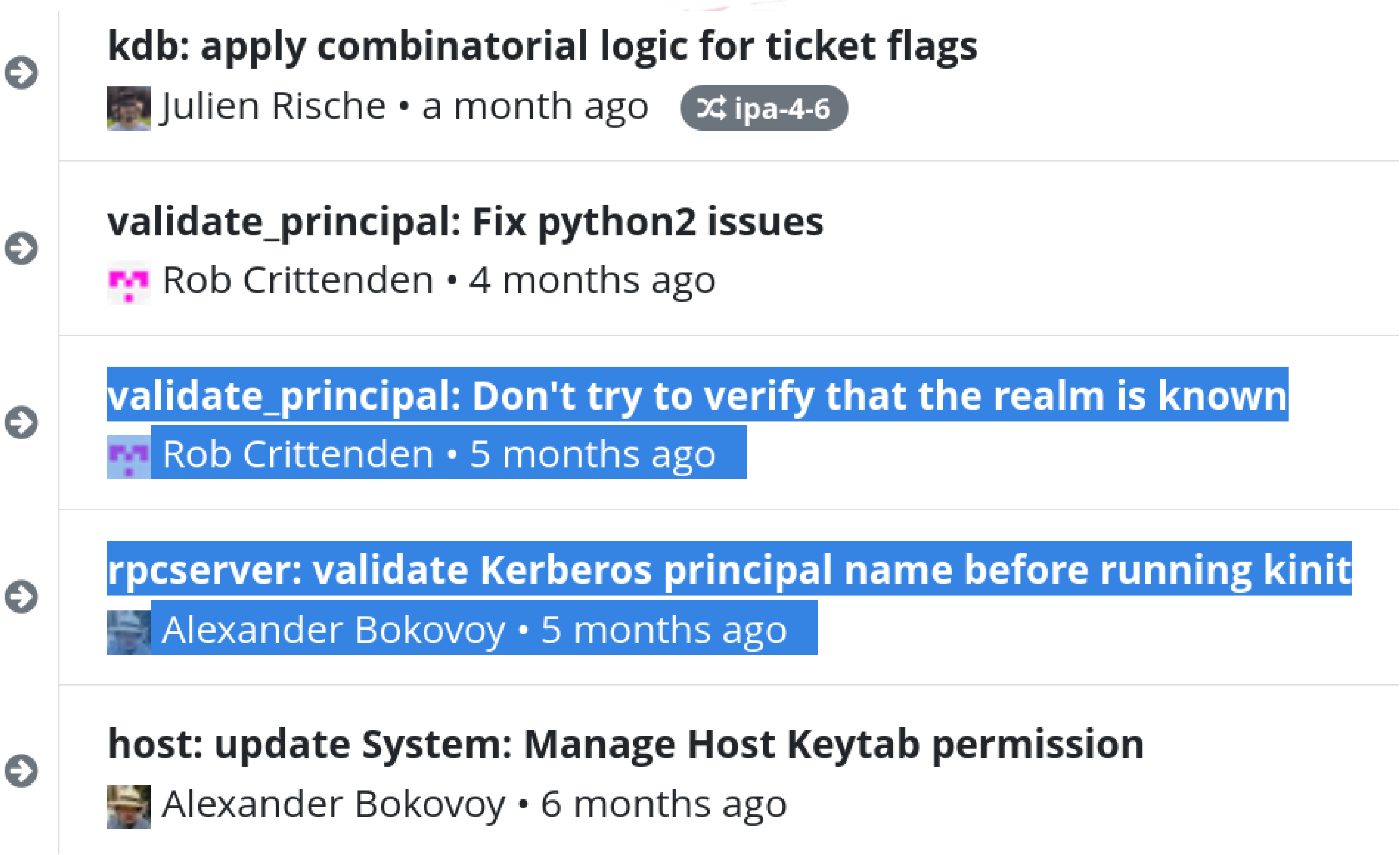
```
- Send no more than 150 cookies per request
- Cap the max length used for a cookie: header to 8K
- Cap the max number of received Set-Cookie: headers to 50

Bug: https://curl.se/docs/CVE-2022-32205.html
CVE-2022-32205
Reported-by: Harry Sintonen
Closes #9048
```

master

tiny-curl-8_4_0 curl-8_8_0 curl-8_7_1 curl-8_7_0 curl-8_6_0 curl-8_5_0 curl-8
curl-8_0_1 curl-8_0_0 curl-7_88_1 curl-7_88_0 curl-7_87_0 curl-7_86_0 curl-7_85_

https://pagure.io/freeipa/commits/ipa-4-6



kdb: apply combinatorial logic for ticket flags

Julien Rische • a month ago ipa-4-6

validate_principal: Fix python2 issues

Rob Crittenden • 4 months ago

validate_principal: Don't try to verify that the realm is known

Rob Crittenden • 5 months ago

rpcserver: validate Kerberos principal name before running kinit

Alexander Bokovoy • 5 months ago

host: update System: Manage Host Keytab permission

Alexander Bokovoy • 6 months ago

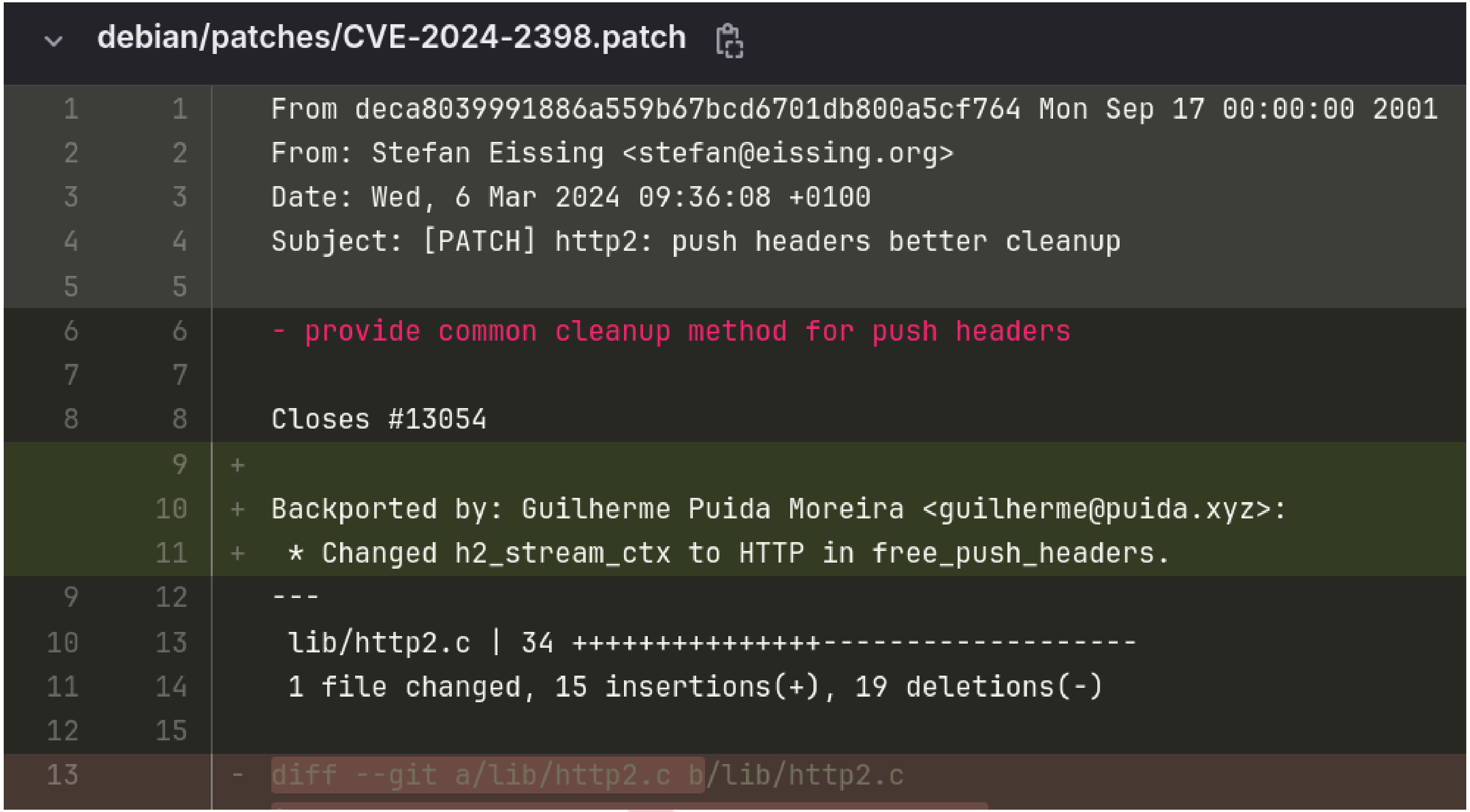
Apply the patches to the Debian packaging

- DEP-3 branch names: debian/bullseye, debian/bookworm...
- Don't let your code editor format the patch
  - Don’t autoremove trailing whitespaces
  - Don’t replace tabs with spaces
- 1 commit introducing the upstream patches without backporting changes
- Add patches to d/series and check if they apply

Modify the patch as needed

- `$ gbp pq --import --time-machine=N`
  - 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 changes
- Overall you should have:
  - 1 commit importing the upstream patch (optional: d/p/series)
  - 1 commit performing the backporting changes (optional: d/p/series)
  - 1 commit for d/changelog

https://salsa.debian.org/debian/curl/-/merge_requests/25



debian/patches/CVE-2024-2398.patch

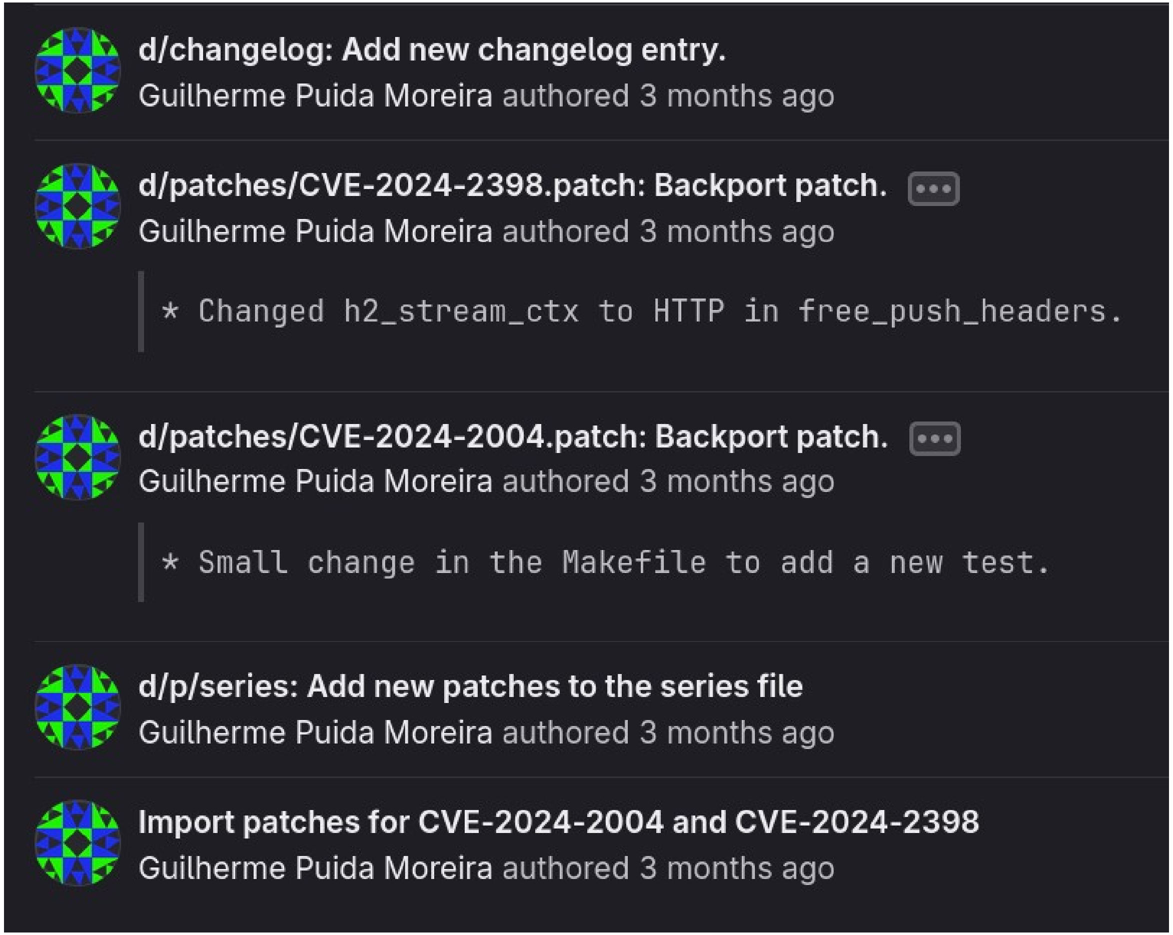
```
  From deca8039991886a559b67bcd6701db800a5cf764 Mon Sep 17 00:00:00 2001
  From: Stefan Eissing <stefan@eissing.org>
  Date: Wed, 6 Mar 2024 09:36:08 +0100
  Subject: [PATCH] http2: push headers better cleanup

  - provide common cleanup method for push headers

  Closes #13054
+
+ Backported by: Guilherme Puida Moreira <guilherme@puida.xyz>:
+  * Changed h2_stream_ctx to HTTP in free_push_headers.
  ---
   lib/http2.c | 34 +++++++++++++++-------------------
   1 file changed, 15 insertions(+), 19 deletions(-)

- diff --git a/lib/http2.c b/lib/http2.c
```

https://salsa.debian.org/debian/curl/-/merge_requests/25



d/changelog: Add new changelog entry.
Guilherme Puida Moreira authored 3 months ago

d/patches/CVE-2024-2398.patch: Backport patch.
Guilherme Puida Moreira authored 3 months ago

```
* Changed h2_stream_ctx to HTTP in free_push_headers.
```

d/patches/CVE-2024-2004.patch: Backport patch.
Guilherme Puida Moreira authored 3 months ago

```
* Small change in the Makefile to add a new test.
```

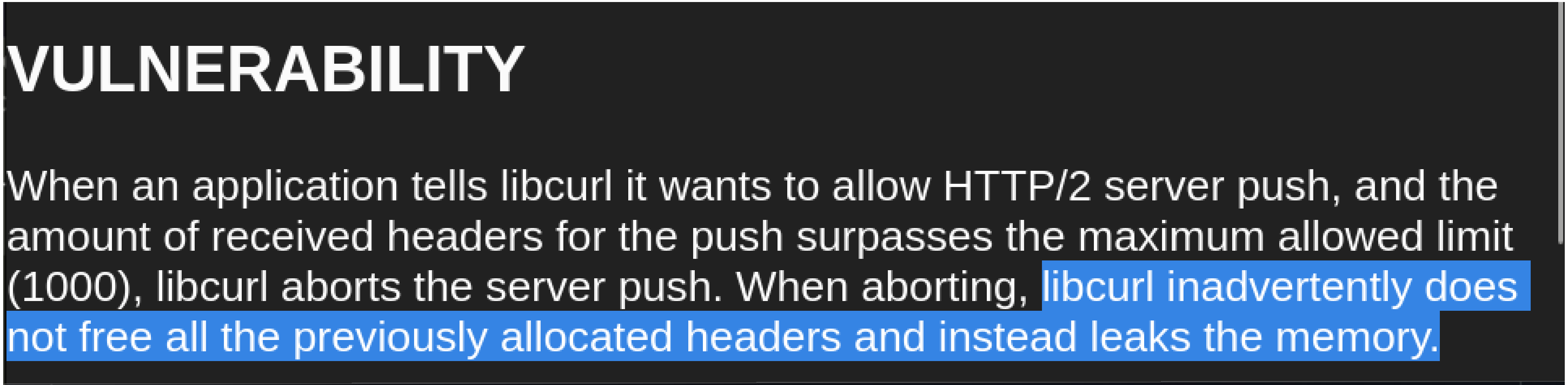
d/p/series: Add new patches to the series file
Guilherme Puida Moreira authored 3 months ago

Import patches for CVE-2024-2004 and CVE-2024-2398
Guilherme Puida Moreira authored 3 months ago

Review the backporting

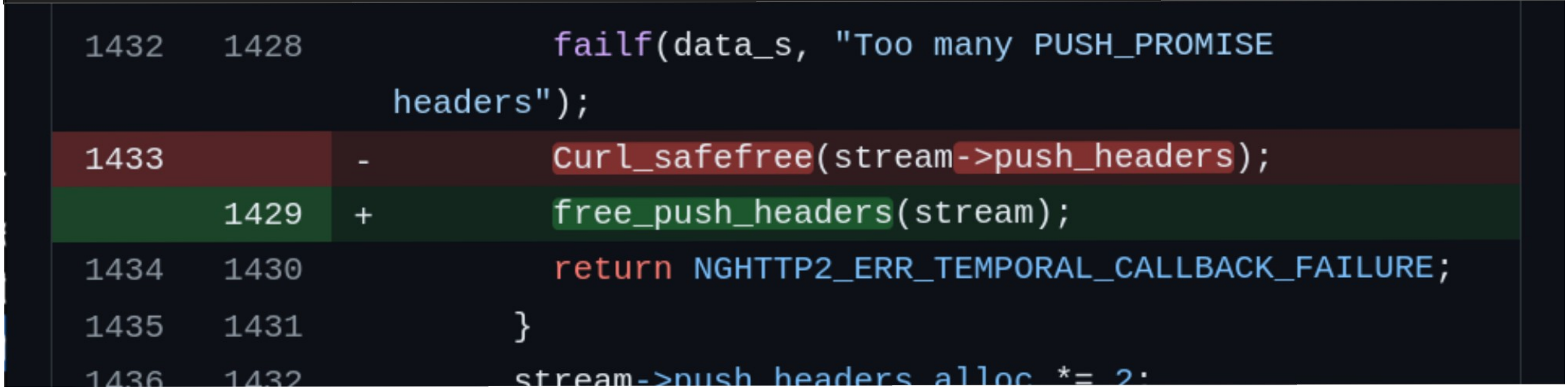
- Backporting changes = diff of a diff
- Reviewing backporting commits saves the day
- If we release a broken fix, a new CVE is created to track it
  - Nobody wants to be a CVE author for this type of CVE
- Pay attention to reordering of hunks
- Question everything

https://curl.se/docs/CVE-2024-2398.html



VULNERABILITY

When an application tells libcurl it wants to allow HTTP/2 server push, and the amount of received headers for the push surpasses the maximum allowed limit (1000), libcurl aborts the server push. When aborting, libcurl inadvertently does not free all the previously allocated headers and instead leaks the memory.



```
            failf(data_s, "Too many PUSH_PROMISE
      headers");
-           Curl_safefree(stream->push_headers);
+           free_push_headers(stream);
            return NGHTTP2_ERR_TEMPORAL_CALLBACK_FAILURE;
          }
          stream->push_headers_alloc *= 2;
```

Test the changes

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

Submit the fix and watch for regressions

- 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

Questions?

I will be around for the whole DebConf, feel free to reach out too

Muito obrigado!

Fixing CVEs on Debian: Everything you probably know already

DebConf24

Busan, Korea

Slides available at samueloph.dev/slides