New issue

Disallow setting an empty list for NPN in CPython 3.9 and earlier #121227

Closed

Labels 3.9 (EOL) stdlib topic-SSL type-security

sethmlarson opened on Jul 1, 2024 · edited by bedevere-app Edits Contributor

Bug report

Bug description:

OpenSSL prior to 3.3.2 had a defect in `SSL_select_next_proto` where invalid values (such as an empty list) would cause a buffer overread (see CVE-2024-5535). The issue can be fixed in CPython by not calling `SSL_select_next_proto` with an invalid value.

This is a low severity vulnerability in CPython and is tracked separately in CVE-2024-5642. CPython 3.10 and beyond removed support for NPN and thus aren't affected by this issue.

CPython versions tested on:

3.8, 3.9

Operating systems tested on:

No response

Linked PRs

- [3.9] gh-121227: Disallow setting an empty list for NPN #137161

sethmlarson added type-bug type-security and removed type-bug on Jul 1, 2024

Eclips4 added 3.9 (EOL) 3.8 (EOL) on Jul 1, 2024

AdrianBunk on Jul 23, 2024

CPython 3.7 to 3.9 are only affected when using OpenSSL < 1.1.1, since CPython >= 3.7 did already drop NPN support with OpenSSL >= 1.1.1 (by accident? see `29eab55` and `9617741`).

CPython 3.8 was released a year after OpenSSL 1.1.1, which makes it unlikely that the vulnerable combination of CPython >= 3.8 and OpenSSL < 1.1.1 would be common.

For Python3 < 3.7 in Debian ELTS I did the big hammer

```
-# define HAVE_NPN 1
+# define HAVE_NPN 0
```

which might also be a reasonable approach for you for the rare affected setups with 3.8 or 3.9?

mcepl added a commit that references this issue on Oct 9, 2024

`[CVE-2024-5642] Switch off NPN support ...` `1036c4b`

StanFromIreland removed 3.8 (EOL) on Jul 28, 2025

bedevere-app mentioned this on Jul 28, 2025

[3.9] gh-121227: Disallow setting an empty list for NPN #137161

picnixz added stdlib topic-SSL on Jul 28, 2025

ambv added a commit that references this issue on Oct 7, 2025

`[3.9] gh-121227: Disallow setting an empty list for NPN (GH-137161)` `a2cdbb6`

StanFromIreland closed this as completed on Oct 7, 2025

StanFromIreland on Oct 7, 2025 Member

I don't know how to mark a CVE as completed.

sethmlarson on Oct 7, 2025 Contributor Author • • •

@StanFromIreland I can update the CVE record. Thanks!

Metadata

Assignees

No one assigned

Labels

3.9 (EOL) stdlib topic-SSL type-security

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

No branches or pull requests

Participants