[CVE-2024-5642] Buffer over-read in SSLContext.set_npn_protocols() for Python 3.9 and earlier

Seth Larson

June 27, 2024 9:09 p.m.

There is a buffer over-read defect in CPython 3.9 and earlier due to not excluding an invalid value for OpenSSL's NPN APIs.

This vulnerability is of severity **LOW**.

CPython doesn't disallow configuring an empty list ("[]") for SSLContext.set_npn_protocols() which is an invalid value for the underlying OpenSSL API. This results in a buffer over-read when NPN is used (see CVE -2024-5535 for OpenSSL). This vulnerability is of low severity due to NPN being not widely used and specifying an empty list likely being uncommon in-practice (typically a protocol name would be configured).

Suggested mitigation is one of the following:

- Upgrade to Python 3.10 or later where NPN isn't supported
- Avoid using NPN via SSLContext.set_npn_protocols()
- Avoid providing an empty list as a parameter to SSLContext.set_npn_protocols()

Attachments:
attachment.html (text/html — 1.0 KB)

0 0

Reply

Show replies by date

674
Age (days ago)

674
Last active (days ago)

List overview

Download

0 comments
1 participants

Add to favorites

TAGS

PARTICIPANTS (1)

Seth Larson