

[Products](#)[Services](#)[Publications](#)[Resources](#)[What's new](#)

[Follow @Openwall on Twitter for new release announcements and other news](#)

[\[<prev\]](#) [\[next>\]](#) [\[day\]](#) [\[month\]](#) [\[year\]](#) [\[list\]](#)

Message-ID: <647e3fc7-f210-48b1-a9a4-48cf330dac54@oracle.com>
Date: Fri, 28 Jun 2024 10:31:31 -0700
From: Alan Coopersmith <alan.coopersmith@...cle.com>
To: oss-security@...ts.openwall.com
Subject: Fwd: [Security-announce][CVE-2024-5642] Buffer over-read in
SSLContext.set_npn_protocols() for Python 3.9 and earlier

Note that in versions of Python that still had NPN support, whether NPN support is built depends on which SSL library/version you build with:
https://github.com/python/cpython/blob/3.9/Modules/_ssl.c#L188-L202

----- Forwarded Message -----

Subject: [Security-announce][CVE-2024-5642] Buffer over-read in
SSLContext.set_npn_protocols() for Python 3.9 and earlier
Date: Thu, 27 Jun 2024 16:09:13 -0500
From: Seth Larson <seth@...hon.org>
Reply-To: security-sig@...hon.org
To: security-announce@...hon.org

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()

View attachment "[Attached Message Part](#)" of type "text/plain" (292 bytes)

[Powered by blists - more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).