Boost_asio TLS Settings Misconfiguration

Name: Boost_asio TLS Settings Misconfiguration

Description: Using the TLS or SSLv23 protocol from the boost::asio library, but not disabling deprecated protocols, or disabling minimum-recommended protocols.

ID: cpp/boost/tls-settings-misconfiguration

Kind: problem

Severity: error

Using the TLS or SSLv23 protocol from the boost::asio library, but not disabling deprecated protocols may expose the software to known vulnerabilities or permit weak encryption algorithms to be used. Disabling the minimum-recommended protocols is also flagged.

Recommendation

When using the TLS or SSLv23 protocol, set the `no_tlsv1` and `no_tlsv1_1` options, but do not set `no_tlsv1_2`. When using the SSLv23 protocol, also set the `no_sslv3` option.

Example

In the following example, the `no_tlsv1_1` option has not been set. Use of TLS 1.1 is not recommended.

```
1 void useTLS_bad()
2 {
3     boost::asio::ssl::context ctx(boost::asio::ssl::context::tls);
4     ctx.set_options(boost::asio::ssl::context::no_tlsv1); // BAD: missing no_tlsv1_1
5
6     // ...
7 }
```

In the corrected example, the `no_tlsv1` and `no_tlsv1_1` options have both been set, ensuring the use of TLS 1.2 or later.

```
1 void useTLS_good()
2 {
3     boost::asio::ssl::context ctx(boost::asio::ssl::context::tls);
4     ctx.set_options(boost::asio::ssl::context::no_tlsv1 | boost::asio::ssl::context::
no_tlsv1_1); // GOOD
5
6     // ...
7 }
```

References

- Boost.Asio documentation.