New issue

Jump to bottom

core: Error out when --require-ssl is specified, but no cert can be loaded #581

Merged **Sput42** merged 2 commits into `quassel:master` from `phuzion:ssl-only` on Jun 18, 2021

Conversation 5 Commits 2 Checks 15 Files changed 1

phuzion commented on Jun 16, 2021 Contributor

As mentioned in #1728, cores launched with the `--require-ssl` flag, but no SSL/TLS certificate available (because the file does not exist, permissions are set incorrectly, the file does not contain a certificate, etc) will effectively be put into a plaintext-only mode, with little more than a small warning on the console to the user. Clients connecting to the core will be given the standard "Unencrypted Connection" warning.

This patch fixes that issue, requiring that cores launched with `--require-ssl` will successfully load a certificate before starting. If the certificate fails to load for any reason during startup, an exception is thrown and the core quits.

Thanks to **@relrod** for the help on this one.

👍 2

`core: Require TLS cert to be loaded if --require-ssl is used` … ✓ `104d01d`

relrod commented on Jun 17, 2021 • edited

This security issue has been assigned `CVE-2021-34825` by MITRE.

justjanne commented on Jun 17, 2021 Contributor

@phuzion has verified that, when reloading certs, the old cert continues being used if the new certs can not be found :)

✓ **justjanne** approved these changes on Jun 17, 2021

View changes

phuzion commented on Jun 17, 2021 Contributor Author

As **@justjanne** mentioned, I did some verification that reloading certs can't put a core into the plaintext-only mode.

To test this, I did the following:

- Set up and launched a core, with a properly configured `quasselCert.pem` file in the configdir.
- Connected to the core to ensure that it works properly
- Disconnected from the core
- Removed the `quasselCert.pem` file from the configdir
- Sent `SIGHUP` (with `pkill -1 quasselcore`) to the core to trigger a configuration reload
- Reconnected to the core

After reconnecting, I was still presented with the previously configured SSL certificate.

digitalcircuit reviewed on Jun 17, 2021

View changes

digitalcircuit left a comment • edited Contributor

This looks sensible! Just some minor questions/nitpicks, some you might not be able to address:

~~Unlike other SSL error messages, no pointer to website~~

~~Now, one could make the argument you'd remove the `--require-ssl` flag to see them, however some distributions include `--require-ssl` by default. I feel we should include the website link if feasible to maintain parity with the other SSL/TLS warning messages.~~

~~See the inline comment with suggestion.~~

This has been fixed!

Reason for exit can be hidden

The exit exception message doesn't seem to be displayed if the `--logfile` option is specified - it's only stored in the log file. However, this applies to all exit exceptions, e.g. `--config-from-environment`. This is not a new bug, but is worthwhile noting.

@Sput42, is it intended for the logging of exit exceptions that result in Quassel exiting to be consumed by a `--logfile`? If I'm understanding correctly, on Debian and Ubuntu even `systemctl status quasselcore.service` won't show this explanatory message unless someone turns on logging to `--syslog`.

Example:

```
user@host:~$ /path/to/quasselcore --require-ssl --listen="127.0.0.1" --configdir="/tmp/qtest/" --logfile="/tmp/qtest/quasselcore.log" --loglevel=Debug
user@host:~$
```

No messages shown. Also applies to `--config-from-environment` , etc.

Should go in release notes - potentially breaking change

It's worthwhile noting this *might* break an existing setup as it turns a prior warning situation into an error. I'm in favor of this - if someone (**which includes package maintainers** - Debian defaults to `--require-ssl` alongside a script to auto-generate certs) sets `--require-ssl` , I feel Quassel *should* error out.

As a result, though, this should likely go in the release notes/ChangeLog when Sput updates them, perhaps with emphasis. If someone deleted the cert and didn't care about encryption, they'll have to remove the flag or put a new cert in.

New string for translators

Minor - this also introduces a new translatable string for the error message.

`src/core/sslserver.cpp` Outdated Show resolved

`Add link to certificate FAQ in --require-ssl error` … ✓ `1fc1282`

Sput42 merged commit **`0674fae`** into `quassel:master` on Jun 18, 2021
15 checks passed

View details

risicle mentioned this pull request on Jan 30

quassel: 0.13.1 -> 0.14.0 NixOS/nixpkgs#157412

Merged

13 tasks

LeSuisse added a commit to LeSuisse/nixpkgs that referenced this pull request on Feb 2

`quassel: apply patches to fix CVE-2021-34825` … `b0c0117`

LeSuisse mentioned this pull request on Feb 2

[21.11] quassel: apply patches to fix CVE-2021-34825 NixOS/nixpkgs#157897

Merged

13 tasks

Reviewers

digitalcircuit

justjanne ✓

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

5 participants