Closed Opened 2 weeks ago by **muffinx**

PKCS12 Passwords

Dear E-Voting PIT Team

I found PKCS12 Passwords in this file:

evoting-solution/source-code/online-voting-mixing/mixnet- spring/src/main/java/com/scytl/products/ov/mixnet/spring /MixingSecureLoggerConfig.java

```
    private static final String CIPHER_PKCS12_PSWD = "649VRY52GXXCNJH48X5F";

    private static final String SIGNATURE_PKCS12_PSWD = "GXXCNJH48X5F649VRY52";
```

These will be later used in the same file:

```
                secureAppender.setCipherPkcs12FileName(CIPHER_PKCS12_CERTIFICATE);
                secureAppender.setCipherPkcs12Password(CIPHER_PKCS12_PSWD);
                secureAppender.setSignaturePkcs12FileName(SIGNATURE_PKCS12_CERTIFICATE);
                secureAppender.setSignaturePkcs12Password(SIGNATURE_PKCS12_PSWD);
```

Since this is a really "deep" part of the Scytl Mixnet, this could be forgotten. I also see the part that its a Logger, but still data could be potentially leaked.

I am happy to contribute to this PIT, and I will try to contact you as "little as possible", since I know that you probably have a lot to do. ;)

Thank you very much for reading my report.

Best Regards

Anthony Schneiter aka. muffinx

---

muffinx @muffinx · 2 weeks ago Guest

Btw. I want to also point out that I have a buddy which helps me, thanks to Jannis Kirschner.

Swisspost @swisspost added In Progress topic: protocol labels 1 week ago

Swisspost @swisspost · 1 week ago Maintainer

Hi Anthony (and Jannis),

Thank you for your input. We will verify this and get back to you.

Kind regards

Swisspost @swisspost · 1 week ago Maintainer

Hello you two,

The contents of the "mixnet-spring" mixing library module are intended to build a standalone application wrapping the mixing library that can be used for purposes like performance testing and scenarios with trusted builds or lower security requirements. They were not intended to be used by dependent projects - other than as an example configuration. Please apologize if this particular library has caused confusion. We will evaluate if would make sense to remove it from the repository or make a clear note in the readme that this is not library used in the productive system In the concrete topic of the secure logger configuration, we are not concerned about this being a threat as we are not consuming such configuration for our control components applications: all control component applications initialize their secure log appenders with their own control component node keys and do not consume the appenders configured in the class under discussion. Reference material:

- ov-control-components/distributed-mixing/distributed-mixing-service/src/main/java/com/scytl/products/ov/channel/cc/mixing /Application.java
- ov-control-components/control-components-commons/src/main/java/com/scytl/products/ov/channel/cc/commons/spring

/AbstractControlComponentApplication.java
- ov-control-components/control-components-commons/src/main/java/com/scytl/products/ov/channel/cc/commons/spring/SecureLoggerConfig.java
- ov-control-components/control-components-commons/src/main/java/com/scytl/products/ov/channel/cc/commons/slogger/SecureLoggerManagerImpl.java
- ov-control-components/distributed-mixing/distributed-mixing-service/src/main/java/com/scytl/products/ov/channel/cc/mixing/spring/MixingConfig.java
- ov-control-components/distributed-mixing/distributed-mixing-service/src/main/resources/log4j.xml

Kind regards

Edited by Swisspost 1 day ago

Swisspost @swisspost closed 1 week ago

Swisspost @swisspost removed In Progress label 1 day ago

Swisspost @swisspost made the issue visible to everyone 1 day ago