12. februar 2019

KOMBIT
Kommunernes it-fællesskab

NOTAT

Sikkerhedsopgradering af anvendersystemer

Indhold

1. Baggrund

KOMBIT ønsker at understøtte højeste generelle sikkerhedsniveauer på alle services der udstilles.

Derfor varsler KOMBIT at der skiftes til et højere sikkerhedsniveau pr 1. juni 2019, og det kan have konsekvenser for nogle anvendersystemer hos kommunerne og ældre Internet browsere der tilgår brugervendte systemer hos KOMBIT.

Formålet med dette dokument er at beskrive omfanget at de eventuelle ændringer de enkelte anvendersystemer kan blive ramt af.

Målgruppen er kommunernes IT ansvarlige, IT arkitekter og anvendersystemer.

1.1 Kontakt

Kontakt helpdesk@serviceplatformen.dk for spørgsmål vedrørende Serviceplatformen

Kontakt sts-support@kmd.dk for spørgsmål vedrørende Støttesystemerne

Kontakt kdi@kombit.dk for generelle og forrretningsmæssige spørgsmål.

2. Omfanget af ændringer

Der er således planlagt følgende ændringer ved pr 1. juni 2019:

2.1 Skift til TLS 1.2

Understøttelse af TLS versioner 1.0 og 1.1 samt krypteringsnøgler markeret som usikre ophører. Dette gælder for alle systemer der kalder element af KOMBIT fælles infrastruktur, herunder specielt

- Serviceplatformen
- Serviceplatformen Administration
- STS Administrationsmodul
- Adgangsstyring for Systemer; Security Token Service
- Beskedfordeler

3. Konsekvenser ved skift til TLS 1.2

De fleste moderne systemer og browsere er uden videre i stand til at benytte TLS 1.2, og vil ikke opleve en ændring.

Der er kendt følgende restriktioner for systemer der tilgår TLS 1.2 services:

3.1 Windows XP og IE8

Klienter der benytter ældre Windows, som eksempelvis Windows XP og Internet Explorer 8 eller tidligere, vil ikke kunne benyttes.

Udfør testen beskrevet i [TLS TEST] for at afgøre om en browser understøtter TLS 1.2

Se 4 Appendiks: Understøttede browsere

3.2 Windows Server 2012 R2 eller tidligere

Systemer der benytter Windows Server 2012 R2 eller tidligere understøtter ikke umiddelbart TLS 1.2 uden at udføre en justering som vist i [Windows]

Bemærk at dette betyder at kommuner der anvender AD FS 3.0, skal udføre disse justeringer, før deres AD FS server kan hente metadata fra Context Handleren.

3.3 Java

Systemer der benytter Java tidligere end 1.6 Update 111, kan ikke benytte TLS 1.2, og skal opdatere Java versionen til update 111 eller senere.

Systemer der benytter Java 1.7 eller 1.6 Update 111 eller senere kan anvende en property som

```
-Dhttps.protocols=TLSv1.2
```

Se den relevante produkts dokumentation for nærmere oplysninger.

Senere version af Java (1.8 og frem) understøtter TLS 1.2 uden videre.

Se [Java]

3.4 .Net

Systemer der benytter .Net anbefales at benytte .Net 4.6 eller senere og benytte en indstilling som

```
System.Net.ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
```

4. Appendiks: Understøttede browsere

Følgende browsere og nyere kan anvende TLS 1.2:

- Google Chrome version 38 eller nyere
- Firefox version 27 eller nyere
- Internet Explorer 11 i Windows 7
- Microsoft Edge alle versioner
- Apple Safari version 7 (iOS X 10.9)
- Apple Safari Mobile version 6 (iOS 6)

5. Appendiks: Referencer

[TLS TEST]	https://www.ssllabs.com/ssltest/viewMyClient.html

[Windows]	https://support.microsoft.com/en-in/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-default-secure-protocols-in-wi https://www.admin-enclave.com/en/articles/windows/305-enable-tls-1-2-on-windows-2012-r2.html
[Java]	https://blogs.oracle.com/java-platform-group/jdk-8-will-use-tls-12-as-default