KOMBIT

Den fælleskommunale infrastruktur

Releasenote for STS2024-11

Releasedato: 15.-16. november 2024

Indholdsfortegnelse

Dokumenthistorik

Dokumentversion	Dato	Beskrivelse
1.0	12. november 2024	Releasenote klar til publicering

Resumé

Støttesystemerne opdateres med fejlrettelser i følgende servicevinduer:

Miljø	**Tidspunkt**	**I servicevinduet kan opleves utilgængelighed og ustabil drift på**	**Servicevinduet påvirker *ikke***
Produktions miljøet	Den 16. november kl. 00.00 til kl. 07.00	Fælleskommunalt Klassifikationssystem Fælleskommunalt Organisationssystem Fælleskommunalt Sags- og Dokumentindeks Fælleskommunalt Ydelsesindeks	Fælleskommunal Adgangsstyring for brugere (Context Handler 1 og 2) Fælleskommunal Adgangsstyring for systemer (Security Token Service 1 og 2) Fælleskommunal Beskedfordeler Fælleskommunalt Organisationssynkroniseringssystem
Eksternt testmiljø	Fra den 15. november kl. 22.00 til den 16. november kl. 05.00	Fælleskommunalt Klassifikationssystem Fælleskommunalt Organisationssystem Fælleskommunalt Sags- og Dokumentindeks Fælleskommunalt Ydelsesindeks	Fælleskommunal Adgangsstyring for brugere (Context Handler 1 og 2) Fælleskommunal Adgangsstyring for systemer (Security Token Service 1 og 2) Fælleskommunal Beskedfordeler Fælleskommunalt Organisationssynkroniseringssystem

Vær særligt opmærksom på

Applikationen ”sts-sagdok-elastic-sync” vil blive flyttet fra afvikling på WildFly-servere til SpringBoot-servere.

Der er i forbindelse med ovenstående ingen ny funktionalitet eller ændring for anvenderne.

Forretningsmæssige ændringer

Denne release indeholder ingen forretningsmæssige ændringer:

ID	Ændring til	Beskrivelse af ændring
n/a	n/a	n/a

Fejlrettelser

Releasen indeholder følgende fejlrettelser.

ID	Ændring til	Uddybet beskrivelse og løsning/status fra leverandøren
CS2428932 Bruger bliver vist 3 gange	Fælleskommunalt Organisationssystem SF1500	Fejl forårsager at der optræder duplikerede brugere på siden *Vis alle medarbejdere.* Tilrettet så der ikke optræder dubletter af brugere.
CS2436634 KMTSAPA-49795 - YdelseListeHent returnerer manglende kle rettigheder, men bruger har rettigheder	Fælleskommunalt Sags- og Dokumentindeks SF1470 Fælleskommunalt Ydelsesindeks SF1490	Hvis kaldet til YdelseListeHentKommune og YdelseListeHentUDKKommune indeholder et token, hvor der er flere serviceaftaler til samme myndighed og samme servicerolle, bliver dataafgrænsningslisterne ikke korrekt lagt sammen til én liste. Det medfører, at det er tilfældigt hvilken en af listerne der bliver benyttet i søgningen og kan derfor resultere i, at data ikke bliver returneret. Ovenstående sammensætning af token er kun set for søgninger fra Borgerblik på data ejet af Udbetaling Danmark, For YdelseListeHent og YdelseListeHentUDKKommune er koden rettet, så der dannes en korrekt dataafgrænsningsliste.
CS2437572 Can't remove addresses	Fælleskommunalt Organisationssystem SF1500	Når adresserelationen er fjernet, gemmes tilstanden ikke, og adressen forbliver synlig. Dette problem forhindrer kommunen i at deaktivere brugeren. Tilrettet så brugeren kan deaktivere brugere.
CS2446587 Problem opening the ORG UI	Fælleskommunalt Organisationssystem SF1500	Indlæsning af organisationshierarkiet tager lang tid, nogle gange op til flere minutter.

		Denne indlæsning er rettet så brugerne ikke skal vente forventelig tid

For listen over kendte udestående fejl henviser vi til Digitaliseringskataloget.dk.

Øvrige rettelser

Releasen indeholder rettelser af fund fra penetrationstesten:

ID	Ændring til	Uddybet beskrivelse og løsning/status fra leverandøren
KL-03 / ORG-01 Insecure file upload potentially leading to csv injection vulnerability	Intern release information	Styrket validering på serversiden: Der er implementeret styrkede valideringsregler for filuploads, især for CSV-filer, for at sikre, at kun forventet indhold som kan uploades.
KL-07 Lack of content-type validation in graphql endpoint	Intern release information	Styrket validering af indholdstype: Der er implementeret styrket validering af indholdstype i headeren (CSP) for alle indgående anmodninger til GraphQL-snitflade. Dette omfatter implementering af sikkerhedsforanstaltninger mod almindelige websårbarheder såsom SQL Injection, XSS og SSRF.
KL-08 / ORG-02 Improper content-type error handling leading to information disclosure	Intern release information	Styrket sikring af fejlsider: Der er implementeret så der på både server- og programside vises generiske fejlmeddelelser i stedet for detaljerede systemoplysninger til slutbrugeren. Disse oplysninger ville potentielt kunne misbruges.
KL-10 / ORG-04 Improper input validation.	Intern release information	Styrket sikring af inputvalidering: Der er implementeret styrket validering, for at alle brugerinput valideres i forhold til et strengt sæt regler for format, type og længde før behandling. Derudover er der forbedringer til fejlhåndtering, der fanger undtagelser og fejl, hvilket forhindrer applikationen i at returnere detaljerede fejlmeddelelser til brugeren.
KL-11 / ORG-05 Incomplete HSTS configuration lacking include subdomains directive	Intern release information	Der er implementeret Strict-Transport-Security-header (HSTS), så den inkluderer includeSubDomains. Dette sikrer, at alle undersider under hovedsiden også udelukkende benytter HTTPS.

KL-12 / ORG-06 Content security policy (CSP) not implemented	Intern release information	Der er implementeret CSP (Content Security Policy) i HTTP-headeren til systemerne.
KL-13 / ORG-07 Cookie configuration missing samesite attribute	Intern release information	Cookieindstillinger: Der er implementeret nye cookieindstillinger som inkluderer SameSite-attributten med værdien ”Strict” hvilket styrker sikkerheden betydeligt.
KL-15 Information exposure through server error message	Intern release information	Der er implementeret så fejlmeddelelser ikke afslører følsomme oplysninger, f.eks. interne implementeringsoplysninger. Disse oplysninger ville potentielt kunne misbruges.