Sårbarheder i AccessManager

Herlev den 12.12.2018

Den 9. oktober blev vi af firmaet ”Improsec” (Improsec.com) varslet om, at de havde fundet nogle sikkerhedsmæssige sårbarheder i AccessManager.

Improsec foretager bl.a. den slags analyser for deres kunder. Hvis de så finder nogen sårbarheder, henvender de sig til programmets ophavsmænd med deres fund.

Henvendelsen er sket under deres ”responsible disclosure” (https://improsec.com/responsibledisclosure/), der kort går ud på at der sættes nogle tidsfrister for hvornår og også hvordan firmaet skal reagere.

Vi har fået 60 dage til at rette programmet, før de vil offentliggøre sårbarhederne.
Selv om det selvfølgelig aldrig er sjovt at blive gjort opmærksom på, at man har et problem, så har hele processen med Improsec været en meget positiv og konstruktiv oplevelse.

Vi har vurderet, at risikoen for at sikkerhedshullerne i AccessManager ville blive udnyttet af nogen ”ondsindede”, var meget lille. Derfor har vi primært knoklet for at lukke sikkerhedshullerne.

Vi vil gerne her understrege, at alle sårbarhederne i AccessManager nu er blevet udbedret, og vi planlægger anbefale jer at opgradere jeres Access Manager til version 6.0.0. Den opdaterede version kan hentes via et link, der sendes pr. e-mail til jer senere i dag

På de følgende sider er de 5 sårbarheder, som Improsec fandt i AccessManager beskrevet en for en med tilhørende løsninger.

Med venlig hilsen

XXXXXXXX
XXXXXXXX
E-mail: XXXXXXXX
Telefon: +45 XXXX XXXX

Ønsker du teknisk support i forbindelse med din AccessManager løsning, bedes du kontakte os på:
E-mail: Support@capmon.dk
Telefon: +45 4485 5065

Gennemgang af de enkelte sårbarheder

Sårbarhed 1 og 2

I AccessManager suiten lå et program “CALRunElevated.exe” der gjorde det muligt at opnå fuld kontrol med den lokale maskine, hvis man afviklede programmet fra en kommando prompt.

1. Der kunne opnås fuld systemadgang via "NT AUTHORITY\SYSTEM", hvis man afviklede programmet med nogle bestemte parametre. Dette var meget nemt at udnytte for en ondsindet bruger eller malware.
2. En almindelig bruger kunne opnå lokal-administratorrettigheder ved at afvikle programmet med bestemte parametre. Dette var også meget nemt at udnytte for en ondsindet bruger eller malware.

Løsning for sårbarhed 1 og 2

“CALRunElevated.exe” var et testværktøj, fra en tidligere version, der ikke mere benyttes i løsningen. Programmet er slettet.

Sårbarhed 3

AccessManager suiten består af en server og en klient.

Serveren indeholder en database med ”whitelistede” applikationer, hvis ”whitelisting” altså benyttes.
En almindelig bruger kan læse denne liste af applikationer. Hvis nogle af disse applikationer ligger i et område, som brugeren har ret til at skrive i, kunne brugeren potentielt erstatte en applikation med en ondsindet applikation.

Dette kunne udnyttes af både brugere og malware.

Løsning for sårbarhed 3.

Tjekke databasen for almindelige brugere og se, om den aktuelle bruger har adgang til at modificere den eksekverbare fil. Hvis brugeren kan dette, får brugeren ikke adgang.

Sårbarhed 4

Det var muligt for en bruger selv at oprette en forbindelse (Named Pipe) til AccessManager Core servicen og derigennem opnå eleverede rettigheder.

Dette kunne nemt udnyttes af ondsindede brugere eller automatiseres af malware.

Løsning for løsning 4

Hver gang der initieres en elevering af brugeren, eller der skal udføres en elevering, tjekkes det, om den aktuelle bruger må blive eleveret via en ”Windows authentication dialog” for at sikre brugerens identitet.
Brugeren kan således ikke længere omgå tjekket ved at prøve at oprette forbindelsen selv.

Sårbarhed 5

En bruger kunne opnå administratorrettigheder ved at afvikle en whitelistet applikation gennem ”Custom App Launcher”. Hvis et kald fejlede, risikerede man, at en bruger blev tilføjet til lokaladmin gruppen, før eleveringsprocessen var startet.

Løsning for sårbarhed 5

Der er nu byttet om på rækkefølgen i tjekket, så der ikke gives lov hvis kaldet fejler.
Dette er kombineret med en ”Windows authentication dialog”, for at sikre brugerens identitet.