POLITIET

Den høyere påtalemyndighet, Riksadvokatembetet
Postboks 2102 Vika
0125 OSLO

Kripos

Deres referanse:	Vår referanse:	Dato:
	20/86507 - 2	22.09.2020

FEIL I SIKRINGER AV IOS-ENHETER VED BRUK AV SIKRINGSVERKTØY

18. mars 2020 ble Kripos varslet fra Cellebrite om at de hadde funnet feil i to av produktene deres – Cellebrite Premium og Cellebrite Physical Analyzer (PA). Feilen ble relatert til DAR-arkiv formatet som har vært benyttet ved sikring av Apple enheter, og feilen oppstod bare ved sikring av telefoner som benyttet APFS som filsystem. Feilen er nå rettet av Cellebrite.

Feilen gikk ut på at PA feiltolket 3 filtidsstempler fra sikringer som var gjort ved bruk av DAR-formatet. Det ble også opplyst at sikringer som ble gjort med Cellebrite Premium ikke inneholdt et fjerde tidsstempel (Time of birth / created)

16. april 2020 mottok NC3 en mail fra dansk NC3 som beskrev feilen nærmere. Undersøkelser som de hadde gjort viste at feilen også omfattet sikringer av Apple produkter som brukte eldre filsystem enn APFS. Videre så det ut til at sikringene var riktige, det vil si at de 3 tidsstemplene som ble hentet ut var riktige, men at disse ble tolket feil når PA ble benyttet til gjennomgang av de sikrede dataene.

30. april 2020 gikk Rigspolitiet i Danmark ut med en pressemelding hvor de opplyste om at en internasjonal leverandør hadde opplyst til dansk politi at det var funnet en feil i en programvare som ble benyttet til å avlese data fra mobiltelefoner og at feilen gikk ut på at enkelte tidsangivelser på filer fra beslaglagte mobiltelefoner kunne være feil. De opplyste videre at feilen var rettet og at det var lite som tyder på at dette har hatt noen betydning i konkrete saker, men at dette skulle bli undersøkt nærmere.

I Danmark er det gjennomgått to saker hvor feilen kunne ha hatt betydning, men i en orientering gitt av Justisministeriet til Folketinget 11. juni 2020 kom det frem at feilen ikke hadde hatt betydning for sakenes utfall.

HVA FEILEN GÅR UT PÅ

Undersøkelse av beslaglagte mobiltelefoner foregår i hovedsak at dataene først blir hentet ut fra telefonen ved bruk av Cellebrite Premium og deretter blir disse dataene tolket av Cellebrite Physical Analyzer (PA) som brukes til gjennomgang av de uthentede dataene.

Feilen går som nevnt ut på at PA feiltolker 3 tidsstempler knyttet til filer som er hentet ut fra telefonen. Tidsstemplene er i seg selv riktige, men de får feil benevnelse i PA. I tillegg var det en mangel ved sikringene ved at tidsstempelet for opprettelse av filene ikke kom med i sikringer som var gjort med Cellebrite Premium.

Nærmere om tidsstempler.

Cellebrite Premium henter nå, etter retting, ut 4 tidsstempler knyttet til filer på mobiltelefoner:

	Engelsk benevnelse	forklaring
1	M - modification	Siste endring av filinnhold
2	A - Access	Siste åpning av fil
3	C – Change of metadata	Siste endring av metadata knyttet til fil
4	Birth / Creation	Da filen ble opprettet

Før retting av feilen hentet Cellebrite Premium ut tidsstemplene nr. 1 til 3 (MAC), men manglet nr. 4.

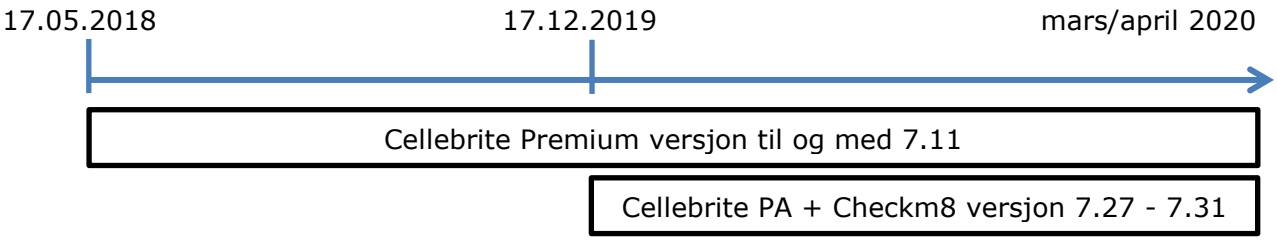
Feilen var at MAC-tidsstemplene fikk feil benevnelse når de ble tolket av PA. Det vil si at tidsstempelet for "change og metadata" (C) kunne bli "Modification" (M) osv. Videre ser det ut til at Cellebrite har misforstått C-change of metadata og trodd at dette tidsstempelet egentlig representerte tidsstempelet for creation og benevnt C-tidsstempelet som created i PA mens dette tidsstempelet i realiteten manglet i sikringen.

Betydningen av feilen/mangelen kommer vi tilbake til nedenfor.

Feilen får litt forskjellig utslag alt etter hvilken versjon av Premium og PA som er blitt benyttet til sikring og gjennomgang av dataene. Etter at feilen er rettet blir alle de 4 tidsstemplene hentet ved bruk av Cellebrite Premium og får riktig benevnelse når de tolkes av PA.

Tidsperiode for feilen

Kripos fikk tilgang til Cellebrite Premium og Physical Analyzer 17. mai 2018. Feilen ved sikringer med DAR-formatet fantes da i programvaren. Fra 17. desember 2019 kunne sikringer med DAR-formatet også gjøres direkte i PA med "checkm8" og feilen vil også være tilstede i disse dataene. Feilen varte frem til den ble rettet i Cellebrite Premium versjon 7.12 og Cellebrite Physical Analyzer versjon 7.32, som begge ble installert på Kripos i månedsskiftet mars/april 2020.



Omfanget av feilen

Sikringer med Cellebrite Premium har i stor grad blitt benyttet på Kripos til sikringer i egne straffesaker og i saker der Kripos har bistått. I tillegg har Oslo politidistrikt Cellebrite Premium.

Checkm8 har ikke blitt benyttet i sak på Kripos, men sikringer med denne programvaren har blitt utført i flere politidistrikt i perioden.

Kripos har igangsatt et arbeid for å innhente oversikt fra politidistriktene over saker hvor det er gjort sikringer med den aktuelle programvaren i den perioden denne hadde feil i tidsstemplene. Dette arbeidet er ikke ferdigstilt og tallmaterialet ettersendes samlet når har kommet inn til Kripos.

I tabellen nedenfor er det en oversikt over de sikringer som Kripos har gjort med Cellebrite Premium i perioden programmet inneholdt feil. Sikringer foretatt som bistand til politidistriktene er ført opp på de politidistriktene som har påtaleansvar i de aktuelle sakene.

Distrikt/særorgan	Antall sikringer	Antall straffesaker
Kripos	20	7
Økokrim	0	0
Oslo politidistrikt	10	10
Øst politidistrikt	12	7
Sør-Øst politidistrikt	10	8
Agder politidistrikt	3	3
Sør-Vest politidistrikt	7	5
Vest politidistrikt	7	4
Innlandet politidistrikt	0	0
Møre- og Romsdal Politidistrikt	1	1
Trøndelag Politidistrikt	9	7
Nordland Politidistrikt	0	0
Troms Politidistrikt	4	4
Finnmark Politidistrikt	0	0

KONSEKVENSER AV FEILEN

Feilen har som sagt medført at filstempler har fått feil benevnelser når de tolkes av PA, og i den grad disse filstemplene er blitt benyttet i den videre analysen av dataene, kan feilen ha hatt betydning.

Det er imidlertid her riktig å moderere dette utgangspunktet noe. For det første er filtidsstempler og feil ved benevnelsen av disse en kjent feilkilde. Misforståelsen av at C-tidsstempelet står for "created" er ikke uvanlig.

For det andre vil feilen i mange tilfeller oppdages når en jobber med tidsstemplene, da det vil være feil i innbyrdes logikk, for eksempel at det som er angitt som "created" vil ha et nyere tidspunkt enn "Modified" eller "Accessed". Videre vil disse tidsstemplene sjelden stå på egne ben som beviser, da det er kjent at disse tidsstemplene kan være usikker vitenskap og avslutningsvis henter Cellebrite PA de fleste tidsstemplene fra innholdet i filene, og ikke MAC-tidsstempler som er knyttet til filenes metadata.

Når det gjelder det siste, kan det her nevnes at tidsstempler knyttet opp mot anrop, SMS, MMS, loggfiler og fra apper vil ikke være berørt av feilen, da disse tidsstemplene hentes fra andre steder en metadataene – dvs de er ikke MAC-tidsstempler.

De tilfellene vi kan tenke oss at feilen kan ha hatt en betydning er hvor filene i seg selv har bevismessig betydning i saken. Dette kan for eksempel være bilder i overgrepssaker hvor tidsstemplene har en betydning i den konkrete saken, eller dokumentforfalskning hvor feil i "modified"-datoen kan ha en betydning.

Videre kan disse tidsstemplene ha en betydning hvor det lages en tidslinje basert på hendelser på en telefon og hvor disse tidsstemplene benyttes. I slike tilfeller kan hendelsene havne på feil sted dersom ett av tidsstemplene det hefter feil ved er benyttet.

Hvor mange straffesaker dette kan ha hatt en betydning i vites ikke, men det er trolig få saker.

AVSLUTTENDE BEMERKNINGER

Cellebrite har laget et flytskjema for hva man kan gjøre for å rette på feilen i beslag som allerede er sikret.

I saker hvor man mistenker at de aktuelle filtidsstemplene har hatt en betydning, bør en ny dekoding med Cellebrite PA versjon 7.32 (eller nyere), gjøres. De 3 filstemplene som er hentet ut av telefonen gjennom sikringen vil da få riktige benevnelser.

Dersom man mener at tidspunktet for "Created/Time of Birth" er av betydning i saken, må det først gjøres en ny sikring med Cellebrite Premium versjon 7.12, eller Cellebrite PA+Checkm8 versjon 7.32, for at dette tidsstemplet skal komme med i sikringen.

Informasjon om dette er gjort tilgjengelig for brukerne av programvaren, slik at saker som fortsatt er under etterforskning ikke blir berørt av feilen.

Med hilsen

Ketil Haukaas
Assisterende sjef Kripos

Dokumentet er elektronisk godkjent uten signatur.