Vedr. IBM Spectrum Protect CVE-2016-8939 sårbarheden:

IBM Spectrum Protect ™ platformen er en af de mest sikre platforme, der tilbydes for cloud backup af kundernes data.
Systemet styres centralt af den enkelte virksomhed, og sikkerheden er helt i top med et af kunden selvvalgt password og 256bit kryptering af de data, der forlader virksomheden og modtages på Front-safes TSM servere / storage platform.
Det er et ekstremt skalerbart system, det benyttes af alle størrelser af kunder - fra kunder med kun én workstation / server – til enterprise kunder med etablering af en / flere frontservere, snesevis af servere - helt op til kunder med en dedikeret TSM infrastruktur med egne TSM servere og båndrobotter.
Alle disse kundetyper kan med stor fordel benytte Front-safes portal: https://tsmportal.com
Hvis udefrakommende får adgang til Front-safes servere, så er det ikke muligt at læse data.
Data opbevares i krypteret form, og kan ikke dekrypteres af Front-safe.

Uautoriseret adgang til virksomhedens data:

Alle IT systemer er sårbare hvis man kan tiltvinge sig adgang til virksomhedens netværk.
Der eksisterer umiddelbart flg. eksempler på dette:

1. Logisk adgang fra internettet,
2. Fysisk adgang til virksomhedens netværk eller servere.

I alle situationer kræver det konstant overholdelse og vedligeholdelse af alle virksomhedens processer og systemer – der skal eks. eksistere processer for adgang til virksomheden, logning af hvem der besøger virksomheden, og overholdelse af regler for udlevering af lånekort.
Alle processer skal konstant vedligeholdes – lige fra regler for fysisk adgang til serverrum, til vedligeholdelse af tildeling af administrative accounts, og endelig til vedligegoldelse af regler på firewall og gennemlæsning af firewall-logs.

TSM Spectrum Protect klienten er som alle andre systemer sårbar, hvis man kan skaffe sig adgang til virksomhedens netværk og videre til eksempelvis registry på klienter / servere.

Det flg. er gældende for alle versioner af IBM Spectrum Protect (tidl: Tivoli Storage Manager):
"TSM Node ID, password og krypteringsnøgle gemmes i registry i en form, der kan udnyttes til ikke autoriseret adgang, så man kan restore TSM data, for ex. stand-alone servere / domain controllere."

Der tegner sig et billede af flg. mulige scenarier:

- **En system administrator forlader sit job:**
  Det er Front-safes anbefaling, at en virksomhed skal have defineret processer for handlinger, når en sys admin stopper.
  De flester ændrer tidligere admins accounts, så de i det mindste bliver disabled, men dette er slet ikke nok, man skal også rette passwords for shared accounts og service accounts.
  De fleste kunder skifter ikke det initielle TSM password, ej heller passwordet for kryptering.
  Node / krypterings password for de enkelte noder skal rettes jævnligt, dette kan udføres vha. Powershell scripts.

- **TSM relateret:**
  Begræns alle brugeres adgang til TSM nøgler i registry, dette kan gøres vha. GPO eller Powershell scripts.
  Node password og encryption password må ikke være kendt af de samme personer
  Overvej kryptering vs. dedub af data, da man ikke både kan kryptere og udføre dedub.

- **Generelle sikkerhedsråd:**
  AD: Benyt en sikkerhedspolitik, der gennemtvinger jævnlig skift af passwords, krav til password kompleksitet og disabling af never ending passwords.
  Brug to – factor – authentication.
  Netværk: Netværk skal være segmenteret.
  TSM netværk skal segmenteres væk fra andre netværk, specielt domain trafik.
  Wifi: Guest netværk skal være adskilt fra company netværk.
  Brug af wifi certifikater.

Flere informationer:

25.5.2017: Controlling access to Windows registry entries for IBM Spectrum Protect backup-archive and data protection clients: http://www-01.ibm.com/support/docview.wss?uid=swg22000998

23.2.2017: Protecting your secrets, one more step to remember:
http://flemmingriis.com/protecting-your-secrets-one-more-step-to-remember/
Flemming Riis viser eksempler på, hvordan man kan restore en server, ved at udnytte denne sårbarhed.

24.2.2017: Bagdøre og datakompromittering via backupsystemer:
https://www.version2.dk/blog/tsm-1073746 *Her er forskellige angrebsscenarier beskrevet*

31.5.2017: IBM Spectrum Protect CVE-2016-8939 Local Information Disclosure Vulnerability:
http://www.securityfocus.com/bid/98783 *Oversigt over de TSM versioner, der er sårbare = alle*

7.6.2017: The enterprise-ready workaround I would have expected from IBM:
https://improsec.com/blog/the-enterprise-ready-workaround-i-would-have-expected-from-ibm
Jakob Heidelbergs gennemgang af beskyttelse af en virksomheds noder vha. GPO´s og Powershell.

12.6.2017: Sårbarhed kendt i måneder: IBM reagerer først efter trussel om offentliggørelse fra V2-blogger: https://www.version2.dk/artikel/saarbarhed-kendt-ni-maaneder-ibm-reagerede-foerst-efter-v2-blogger-truede-med Version2´s gennemgang, med hele historikken.

Helge Hellesøe
Support consultant

hhe@front-safe.dk

+45 70 27 25 90

www.front-safe.dk