

Oppdatering 8. mai 2021

Onsdag 05.mai 2021, opplevde Volue ASA et omfattende dataangrep mot Volue Technology (Volue). Angrepet mot Volue kom i form av et løsepengevirus (ransomware) og ble gjennomført ved bruk av et såkalte Ryuk virus. Dette er et virus som normalt brukes til å angripe store offentlige aktører med Microsoft Windows systemer.

Operasjonen Stop & Recover til Volue har fortsatt siden forrige oppdatering. Dette for å kartlegge effekten og omfanget av angrepet på selskapets produkter og tjenester. I løpet av de siste 24 timene har vi klart å kartlegge en stadig større del av vektor og tidspunkt for angrepet. Gjennom dette arbeidet har vi fått en bedre oversikt over hvilke produkter og tjenester som har blitt påvirket av angrepet.

Vi kan bekrefte at angrepet omfattet systemer med powel og onpowel.com domener. Angrepet ser ikke ut til å ha berørt systemer på Volue domene. Den siste tiden har en stor andel av de ansatte i Volue jobbet hjemmefra og ikke vært koblet til Powel nettverket via VPN. Disse er derfor ikke berørt av angrepet.

Volue har innledet et nært samarbeid med kraftbransjens egen ekspertgruppe, KraftCERT (Computer Emergency Response Team) og vil dele teknisk informasjon om angrepet med denne gruppen. KraftCERT har partnere i andre europeisk land og vil også kunne bistå kunder utenfor Norge. Kunder kan ta direkte kontakt med KraftCERT på cert@kraftcert.no og telefon: +47 940 32 443.

En viktig prioritert for Volue er å oppdatere våre kunder på status til applikasjoner påvirket av angrepet. Våre undersøkelser viser så langt at den store majoriteten av Volue Technology's ("Powel") portefølje og applikasjoner ikke har blitt berørt. Undersøkelsene er pågående, men vi har stor grunn til å tro at applikasjoner som er delt på [Recovery Status page on volue.com](#) ikke er komprimert og således å betrakte som operasjonelle. Vi vil oppdatere listen over dette kontinuerlig.

Servere og systemer som ble påvirket av angrepet inneholdt blant annet data fra kundene til Volue og vi har på det nåværende tidspunkt ikke klart å få tilgang til disse. Da vi ikke er ferdig med våre undersøkelser rundt angrepet, er det for tidlig å anslå omfanget av data som er omfattet av angrepet. Vi har imidlertid ingen indikasjoner på at filene som inneholder data fra kundene, har blitt tatt ut eller flyttet til eksterne severere. Alle berørte kunder har blitt informert om saken. Hendelsen har også blitt rapportert til Datatilsynet.

IT teamene til Volue har arbeidet med å isolere og siden gjenoppbygge og gjenopprette den aktuelle infrastrukturen. Dette arbeidet har pågått parallelt med undersøkelsene av angrepet. Teamene til Volue gjennomfører også katalogisering og vurdering av applikasjoner og infrastruktur.

Åpenhet og kommunikasjon er grunnleggende for Volue. Vi gjennomfører daglige webmøter hver morgen kl. 09.30 og det neste webmøtet vil bli gjennomført på søndag, 9. mai, kl. 09.30

For å delta på de daglige web møtene kan du registrere deg [her](#).
Dagens sesjon kan du finne [her](#).

For mer informasjon vennligst kontakt Volue [support](#).