

Water & Community

Oppdatering på dataangrepet og produkter

12. mai 2021 - 13:00 CEST

5. mai 2021 opplevde Volue et omfattende dataangrep mot Volue Technology, tidligere Powel. Angrepet kom i form av et løsepengevirus (ransomware) og ble gjennomført ved bruk av en såkalte Ryuk-gruppe. Umiddelbart etter angrepet iverksatte Volue operasjonen 'Stop & Recover'. Denne operasjonen har blitt kontinuerlig utvidet samtidig som vi har styrket samarbeidet med myndighetene og eksterne sikkerhetspartnere.

Gjennom våre avanserte sikkerhetssystemer har vi hatt tilgang til store mengder data og logger. Dette har gitt oss god innsikt i tidslinjen for angrepet, inkludert angripernes forberedelse, rekognosering og faktiske angrep. All denne informasjonen har blitt delt med KraftCert, som kombinert med sine egne undersøkelser, har igjen har delt informasjonen med sitt nettverk og samarbeidspartnere, inkludert KommuneCert.

Vi har fortsatt ingen indikasjoner eller bevis som tilsier at data, verken personopplysninger eller infrastruktur-kritiske, er på avveie. Dette er et område vi tar svært seriøst, og vi vil fortsette våre undersøkelser slik at vi med høyest mulig grad av sikkerhet kan utelukke at data er på avveie.

Vi vet at løsningene våre er viktige for dere, og at dataangrepet har skapt store utfordringer. Flere har vært bekymret for dataene sine – om de var ødelagt, utilgjengelig eller kanskje på avveie, blant annet dataene i Gemini VA. Vi har backup av Gemini VA-dataene, og backupen lå trygt under angrepet. Vi har også backup av alle andre data i vårt skymiljø. Alle data er nå klargjort for bruk.

Tidlig i prosessen anbefalte vi dere å endre passord for Volue-brukere med tilgang til tjenester, servere, eller domener. Dere kan enkelt øke sikkerheten ved å øke lengden på passord, unngå å dele passord, samt unngå å ha fellesbrukere. Alle bør ha egne, personlige brukere. Et av mange sikkerhetstiltak vi gjør nå, er å innføre to-faktor-autentisering på enda flere tjenester, som innebærer en ekstra sikkerhetsmekanisme i tillegg til brukernavn og passord. For eksempel kan det være i form av en kode tilsendt på mobilen, som du må taste inn for å komme inn i en applikasjon.

Det har vært en del spørsmål rundt hvordan våre kunder skal kommunisere og samarbeide med våre ansatte. Per i dag er det email, Teams, Teamviewer og telefon som gjelder. Vi anser nå også fildeling mellom Volue sine ansatte og kunder som trygt. Vi vil på et senere tidspunkt dele mer informasjon om hendelsen og ikke minst vår læring i denne prosessen. Vi er en del av det samme nettverket, og sikkerhet og sårbarheter i forhold til denne type angrep er noe som angår oss alle.

Vi er svært opptatt av å gi god og så fullstendig informasjon som mulig til våre kunder. Vi vil fortsette å holde dere løpende orientert om utviklingen i denne saken.

Water & Community produktstatus 12. mai 2021

Status per 12. mai 2021

● Anses som trygg
● Arbeid pågår

Løsning	Status	Kommentar
Gemini Varsling		Mangler VA-kart
Gemini Melding		
Gemini Water Alert		
Gemini Privat		Mangler arkivintegrasjon sky , skissefunksjon og VA-kart
Datamann brann/feie		
LER/Gravemelding DK (Sky)		
Gemini VA (Lokal)		
Gemini Portal (Lokal)		
Gemini VA (Sky)		2-faktor autentisering satt opp
Gemini Portal (Sky)		Vil komme krav om 2-faktor autentisering
Gemini Ledningsfornvelse		
Geonis DK (Sky)		
Gemini Datakvalitetsanalyse		

[Her](#) kan dere se et opptak av dagens webcast.

[Her](#) finner dere instruksjoner for å rapportere angrepet til Datatilsynet

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