

Update 8 May 2021 - 11:00 CEST

On 5 May 2021, Volue was subject to a cyberattack impacting Volue Technology ("Powel"). The ransomware attack was caused by Ryuk, a type of malware usually known for targeting large, public-entity Microsoft Windows systems.

Since the last update, the operation Stop & Recover has continued assessing the impact status for Volue's products and services. During the last 24 hours, we have been able to clarify more of the vector and timing of the attack. We have been able to obtain a better overview on the status of products and services that has been affected by the attack.

We can confirm that attacks occurred on systems with the powel and onpowel.com domains. It doesn't appear the Volue domain was compromised. During this period, the vast majority of Volue employees were working from home, not connected to the Powel network via VPN and thus not susceptible.

Moreover, Volue have initiate a close cooperation with the Computer Emergency Response Team for the power industry ([KraftCert](#)) and will share relevant technical information about the attack with the group. KraftCert cooperates with partners in other European countries and will assist also customers outside of Norway. Volue customers may contact KraftCert directly at email: cert@kraftcert.no or phone +47 940 32 443.

Another priority is to update customers on the status of application impacted by the attack. Based on our investigations, it appears likely that the vast majority of Volue Technology's ("Powel") portfolio and applications have not been compromised. These investigations are ongoing, but we believe we can say with a high degree of confidence that applications shared on the [Recovery Status page on volue.com](#) are not compromised and as such are considered operational. We will update the list continuously.

The servers and systems which are affected did, however, contained data from customers of Volue and are currently inaccessible. The total amount of personal data concerned is still unclear, as we have not finalised our investigation of the scope of the attack. We have however no indication to believe that any files containing personal data has been extracted and transferred to any third parties. All customers that have been affected have been informed. We have reported the incident to the National Supervisory Authority in Norway (Datatilsynet).

Engineering and IT teams at Volue have been isolating and then rebuilding and restoring infrastructure, even while the investigation is ongoing. In addition, the teams are cataloguing and assessing applications and infrastructure.

Transparency and communication are important for Volue. In our daily status webcasts, held every morning at 9.30 am followed by a news updated, we will inform you about the current situation. The next webcast is streamed on Sunday, 9 May, 9.30 am.

Register for the daily update webcast [here](#).

View todays recorded session [here](#).

For more information, please contact the Volue [support](#).