# Energy giant Shell discloses data breach after Accellion hack

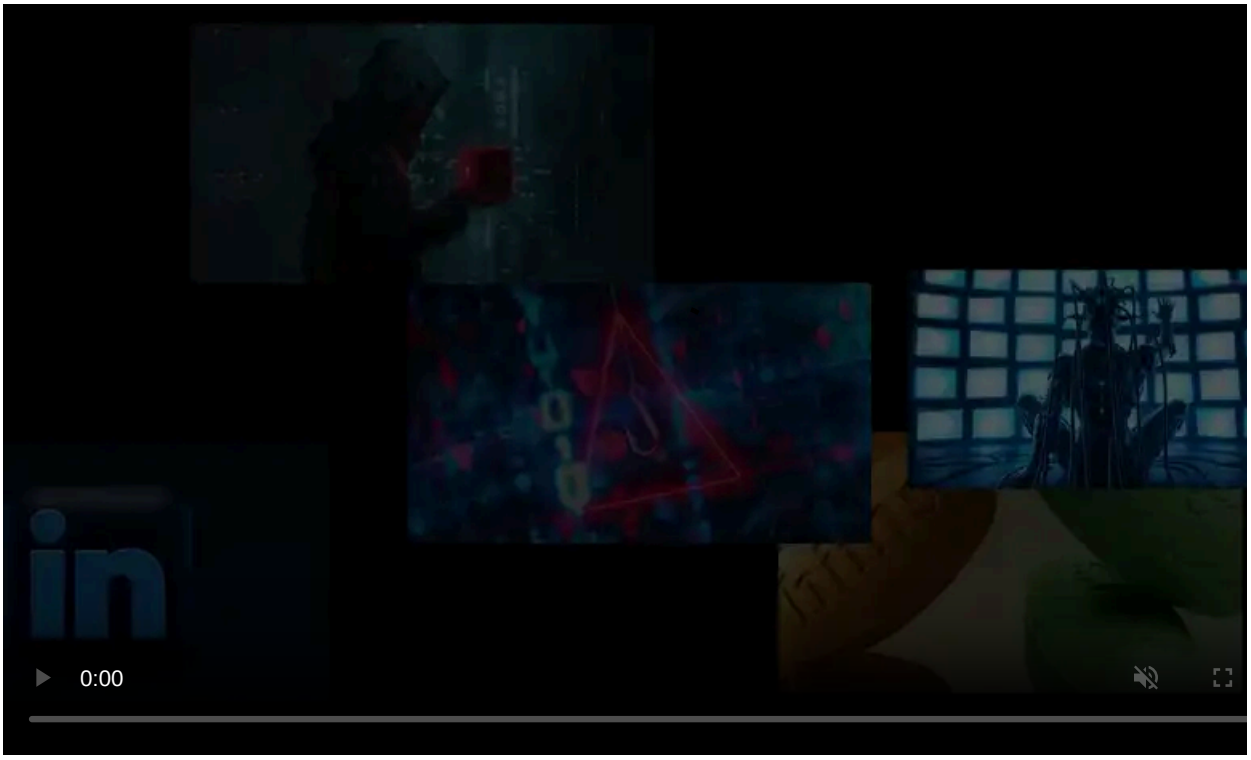
By Sergiu Gatlan

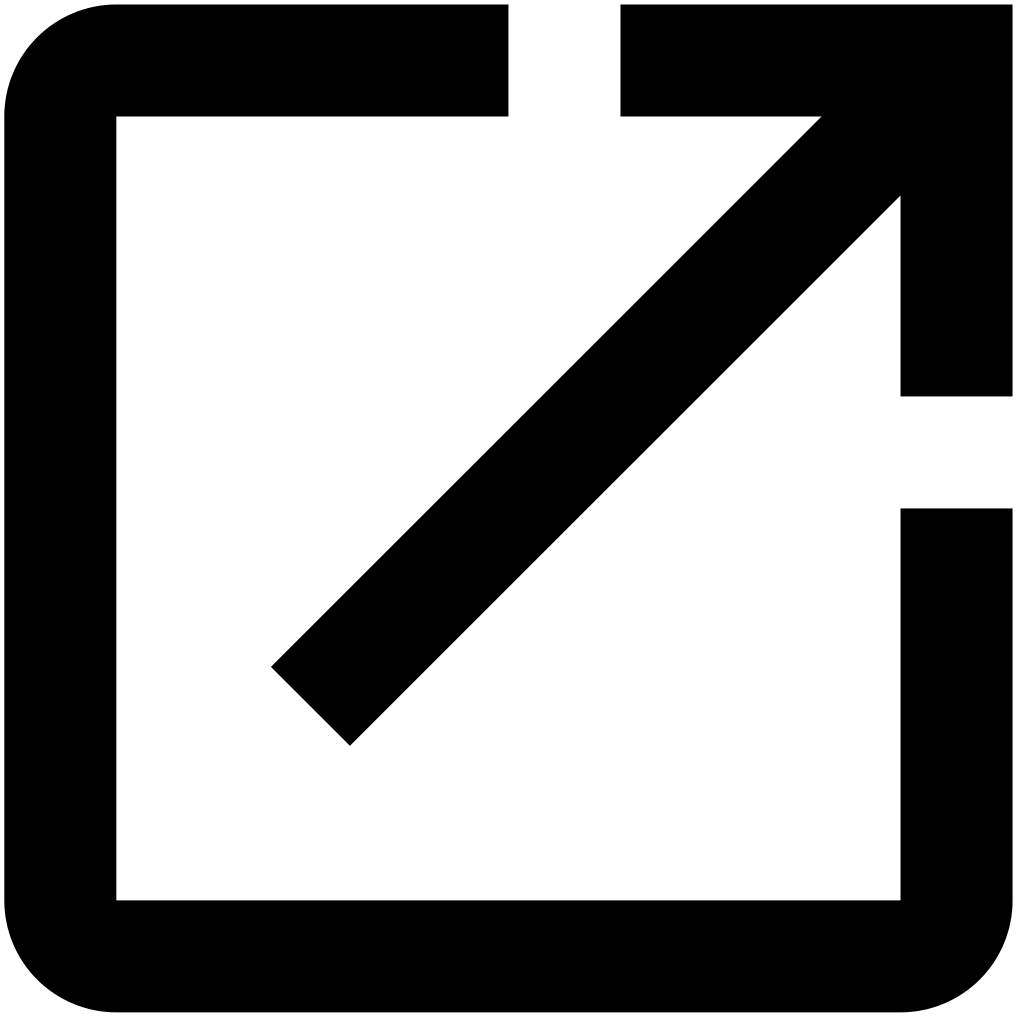
Published: 2021-03-22 · Archived: 2026-04-05 18:20:58 UTC


*Image: Nicholas Jeffway*

Energy giant Shell has disclosed a data breach after attackers compromised the company's secure file-sharing system powered by Accellion's File Transfer Appliance (FTA).

Shell (short for Royal Dutch Shell plc) is a multinational group of petrochemical and energy companies with more than 86,000 employees in over 70 countries.


0:00



It is also the fifth-largest company in the works based on its 2020 revenue results according to Fortune's Global 500 rankings.

## Attack didn't affect Shell's network

Shell disclosed the attack in a public statement published on the company's website last week and said that the incident only affected the Accellion FTA appliance used to transfer large data files securely.

"Upon learning of the incident, Shell addressed the vulnerabilities with its service provider and cyber security team, and started an investigation to better understand the nature and extent of the incident," Shell said.

"There is no evidence of any impact to Shell's core IT systems as the file transfer service is isolated from the rest of Shell's digital infrastructure."

Shell also reached out to relevant data authorities and regulators after discovering that the attackers gained access to files transferred using the compromised Accellion FTA appliance.

According to the company, some of the data accessed during the attack belongs to stakeholders and Shell subsidiaries.

"Some contained personal data and others included data from Shell companies and some of their stakeholders," the statement reads.

"Shell is in contact with the impacted individuals and stakeholders and we are working with them to address possible risks."

> Cyber security and personal data privacy are important for Shell and we work continuously to improve our information risk management practices. We will continue to monitor our IT systems and improve our security. We regret the concern and inconvenience this may cause affected parties. — Shell

## Clop ransomware gang and FIN11 behind series of Accellion hacks

While the attackers' identity was not disclosed in Shell's statement, a joint statement published by Accellion and Mandiant last month shed more light on the attacks, linking them to the FIN11 cybercrime group.

The Clop ransomware gang has also been using an Accellion FTA zero-day vulnerability (disclosed in mid-December 2020) to compromise and steal data from multiple companies.

Accellion said that 300 customers used the 20-year-old legacy FTA software, with less than 100 of them being breached by the Clop ransomware gang and FIN11 (the cybercrime groups behind these attacks).

Less than 25 victims appear "to have suffered significant data theft," according to Accellion.

BleepingComputer has reported breaches affecting multiple organizations following attacks targeting Accellion FTA, including cybersecurity firm Qualys, the supermarket giant Kroger, the Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), Singtel, QIMR Berghofer Medical Research Institute, and the Office of the Washington State Auditor ("SAO").

Five Eyes members have also issued a joint security advisory last month about ongoing attacks and extortion attempts targeting orgs using unpatched Accellion File Transfer Appliance (FTA) versions.

BleepingComputer has reached out to Shell for comment but has not heard back.

---