Morgan Stanley reports data breach after vendor Accellion hack

bleepingcomputer.com/news/security/morgan-stanley-reports-data-breach-after-vendor-accellion-hack/

Sergiu Gatlan

By
Sergiu Gatlan

- July 8, 2021
- 09:19 AM
- 0

Image: Morgan Stanley

Investment banking firm Morgan Stanley has reported a data breach after attackers stole personal information belonging to its customers by hacking into the Accellion FTA server of a third-party vendor.

Morgan Stanley is a leading global financial services firm providing investment banking, securities, wealth and investment management services worldwide.

The American multinational company's clients include corporations, governments, institutions, and individuals in more than 41 countries.

Encrypted files stolen together with decryption key

Guidehouse, a third-party vendor that provides account maintenance services to Morgan Stanley's StockPlan Connect business, notified the investment banking company in May 2021 that attackers hacked its Accellion FTA server to steal information belonging to Morgan Stanley stock plan participants.

The Guidehouse server was breached by exploiting an Accellion FTA vulnerability in January before the vendor patched it within five days of the fix becoming available.

Guidehouse discovered the breach in March and the impact to Morgan Stanley customers in May, when it notified the financial services company of the incident and that no evidence was found of the stolen data being disseminated online by the threat actors.

"There was no data security breach of any Morgan Stanley applications," Morgan Stanley said in data breach notification letters sent to impacted individuals.

"The incident involves files which were in Guidehouse's possession, including encrypted files from Morgan Stanley."

However, even though the stolen files were stored in encrypted form on the compromised Guidehouse Accellion FTA server, the threat actors also obtained the decryption key during the attack.

Morgan Stanley says that the documents stolen during this incident contained:

- Stock plan participants' names
- Addresses (last known address)
- Dates of birth
- Social security numbers
- Corporate company names

The company added that the files stolen from Guidehouse's FTA server did not contain passwords information or credentials that the threat actors could use to gain access to impacted Morgan Stanley customers' financial accounts.

"The protection of client data is of the utmost importance and is something we take very seriously," a Morgan Stanley spokesperson told BleepingComputer. "We are in close contact with Guidehouse and are taking steps to mitigate potential risks to clients."

Clop gang and FIN11 behind series of Accellion hacks

While the attackers' identity was not disclosed in Morgan Stanley's data breach notification, a joint statement published by Accellion and Mandiant from February shed more light on the attacks, directly linking them to the FIN11 cybercrime group.

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

Accellion has said that roughly 300 customers used the 20-year-old legacy FTA software, with less than 100 of them being breached in these attacks.

Starting in January, BleepingComputer has reported multiple data breaches impacting companies and organizations after their Accellion FTA servers were compromised, allowing the cybercrime groups to exfiltrate sensitive information.

So far, these threat actors have hit energy giant Shell, cybersecurity firm Qualys, the Reserve Bank of New Zealand, Singtel, supermarket giant Kroger, the Office of the Washington State Auditor ("SAO"), the Australian Securities and Investments Commission (ASIC), and multiple universities and other organizations.

In February, Five Eyes members have also issued a joint security advisory on these attacks and extortion attempts.

Related Articles:

General Motors credential stuffing attack exposes car owners info

Ransomware attack exposes data of 500,000 Chicago students

Engineering firm Parker discloses data breach after ransomware attack

Coca-Cola investigates hackers' claims of breach and data theft

French hospital group disconnects Internet after hackers steal data