Accellion Compromise Impacts Many Targets Including Healthcare Organizations

Executive Summary

Accellion, a managed service provider focused on collaboration and secure file sharing, was recently compromised in an attack which has impacted their customers. It is believed that up to 100 of their customers were part of a secondary attack and up to 25 of those had a significant amount of their data stolen. The root cause of the breach was the exploitation of multiple vulnerabilities in their legacy File Transfer Appliance (FTA). The recommended actions for any organization, whose infrastructure includes FTAs, are to first determine if your organization has been compromised (and if so, to mitigate it) and second, to upgrade the FTA technology.

Report

Accellion was first found to be compromised in mid-December, 2020. The compromise involved a zero-day SQL injection vulnerability in their File Transfer Appliance (FTA), a 20-year-old legacy product used by corporations around the world. After patching the vulnerability, further investigation revealed additional vulnerabilities (see below for details). The attackers appear to be financially-motivated cybercriminals and although 100% attribution has not been made, they are tracked as UNC2564 and are believed to be affiliated with FIN11 and the Clop Ransomware operators, if not carried out by them directly. The attackers stole data and threaten to post it on the dark web if they are not paid the sum they demand. An example of an extortion note is below.

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

Figure 1: Extortion note (source: FireEye)

Not all of the victims of this attack are known to the public at this time. Among the ones that are public are supermarket giant Kroger (including pharmacy and other health-related data), Singtel, QIMR Berghofer Medical Research Institute, Reserve Bank of New Zealand, the Australian Securities and Investments Commission (ASIC), and the Office of the Washington State Auditor, the technical services company ABS Group, the law firm Jones Day, a Fortune 500 science and technology corporation Danaher, the geo-data specialist Fugro and the University of Colorado, among others.

The following CVEs have since been reserved for tracking the recently patched Accellion FTA vulnerabilities:

CVE-2021-27101 – SQL injection via a crafted Host header

CVE-2021-27102 – OS command execution via a local web service call
CVE-2021-27103 – SSRF via a crafted POST request
CVE-2021-27104 – OS command execution via a crafted POST request

Recommended Actions

The Department of Health and Human Services recommends two actions for any organization that includes Accellion FTAs as part of its enterprise infrastructure: First, conduct a thorough investigation to determine if the organization in question was part of the compromise, and if so, work to characterize, contain and eradicate the threat as soon as possible. Further technical details on the attacks, including tactics, techniques, and procedures, indicators of compromise (IOCs) as well as other information can be found in this FireEye blog (also included in references). We also recommend, as with all IOCs, an exhaustive search of all available sources be carried out and operationalization is aligned to the risk management plan. The second recommended action for any organization that includes Accellion FTAs as part of its enterprise infrastructure is to replace it. Accellion's File Transfer Appliance is a 20-year-old product that will reach its end-of-life at the end of April. Accellion strongly recommends that FTA customers migrate to KiteWorks, which is their enterprise content firewall platform which they state is built on an entirely different code base. This is one of many available products in the market that may meet requirements.

References

Global Accellion data breaches linked to Clop ransomware gang
https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/

Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion
https://www.fireeye.com/blog/threat-research/2021/02/accellion-fta-exploited-for-data-theft-and-extortion.html

Accellion FTA Zero-Day Attacks Show Ties to Clop Ransomware, FIN11
https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/

The Accellion Mess: What Went Wrong?
https://www.databreachtoday.com/blogs/accellion-mess-what-went-wrong-p-2989

Accellion FTA
https://www.accellion.com/products/fta/

Accellion FTA end-of-life announcement
https://www.accellion.com/sites/default/files/resources/fta-eol.pdf