Accellion FTA Attack Customer FAQs

Attack Scope, Timeline and Response

What systems were affected by this incident?

The incident impacted a subset of the 320 customer systems of our File Transfer Appliance (FTA) software. The incident did not affect our flagship Kiteworks® content firewall platform, which is built on an entirely different codebase.

What gives you confidence that the incident has been contained and remediated?

Accellion engaged Mandiant to conduct an exhaustive investigation of the incident and review of the FTA software for any other remaining vulnerabilities. Mandiant has issued a full report detailing its work, explaining that they have confirmed that the vulnerabilities explained in FAQs below were the only vulnerabilities involved in the attack, and that the patches issued by Accellion fully resolve those vulnerabilities. At this time, all known vulnerabilities in the FTA software have been closed. Accellion has also announced end of life for the FTA platform and is working closely with clients to move them to our flagship Kiteworks® content firewall platform, which is built on an entirely different codebase.

When did you discover the attacks on FTA clients, and how soon did you respond?

The attacks were based on two different exploits—one that was discovered and promptly addressed in December 2020 ("December Exploit"), the other that was discovered and promptly addressed in January 2021 ("January Exploit").

December Exploit: We first learned of anomalous activity linked to the December Exploit on December 16. Every customer's FTA system has a built-in anomaly detector that sends the customer an email alert if it detects anomalous behavior on the system. After a customer received such an alert on December 16, the customer requested Accellion support. We promptly investigated and determined that the anomaly was due to malicious activity. Accellion identified two previously unknown vulnerabilities in FTA (CVE-2021-2701 and CVE-2021-2704) that the attacker had chained together to form a sophisticated exploit that enabled the attacker to download files from the FTA system without being authenticated. Accellion developed and released a patch for the vulnerabilities involved in this exploit (FTA-9_12_380) on December 20 and notified all FTA customers to update their systems immediately. Accellion proactively applied the patch to all FTA systems for clients that subscribe to Accellion-arranged hosting. This patch was sufficient to eliminate the vulnerabilities involved in the December Exploit. As a further security measure, Accellion released an additional security update (FTA-9_12_401) on December 23, which increased the frequency of anomaly detector checks from once per day to once per hour. A third update (FTA-9_12_411) was released on December 24, to fix minor usability issues introduced by the prior two security patches.

January Exploit: On January 22, we learned through multiple customer service inquiries of different anomalous behavior, which was indicative of a new exploit. We promptly issued an urgent security alert to FTA customers advising them to shut down their FTA systems immediately. Upon further investigation, we found that this second exploit relied on two different, previously unknown vulnerabilities (CVE 2021-2702 and CVE-2021-2703), again chained together to form a sophisticated exploit that allowed the attacker to download files from the FTA system without authenticating. The earliest evidence we have seen of any use of this exploit is from January 20, 2021.

We have provided a timeline of the two attacks reflecting the discovery of the exploits, the issuance of software patches, and related communications to our clients.

When and how were customers notified there was a problem?

December Exploit: FTA customers were first notified of the need to patch their systems on December 20, when the first patch was released. An email alert was sent to FTA customers describing the software update as critical and time-sensitive, and strongly encouraging customers to update as soon as possible. In addition, Accellion customer support proactively reached out to customers individually by email and phone. Subsequent email alerts were sent out on December 23, notifying customers of the second update, as well as on January 4, reminding customers about the release of these patches. Both emails again described the issue as critical and time-sensitive, and strongly encouraged customers to update as soon as possible.

January Exploit: On January 22, the same day that we discovered the exploit involved in the January Exploit, we sent an urgent critical security update to FTA customers, explaining that there was an active exploit in the FTA software and strongly encouraging customers to shut down their FTA systems immediately. On January 25, we emailed all FTA customers to advise them of the patch for the vulnerabilities involved in the exploit, which we urged customers to apply as soon as possible.

Have all vulnerabilities been fully resolved?

The patches issued by Accellion effectively close all known vulnerabilities associated with both the December Exploit and the January Exploit. Accellion reported the vulnerabilities to the Common Vulnerabilities and Exposures (CVE) database under the following identifiers:

- CVE-2021-27101 (used in December Exploit)
- CVE-2021-27104 (used in December Exploit)
- CVE-2021-27102 (used in January Exploit)
- CVE-2021-27103 (used in January Exploit)

How can you be sure unauthorized actors were not able to use the exploits as a backdoor into our systems?

The two exploits at issue were specific to the FTA software and were specifically engineered to help identify and exfiltrate files stored in a customer's FTA system. Based on the review of logs from certain customers, no evidence was found of methods or attempts to move laterally into a customer's network.

Were Accellion corporate systems compromised?

No. Accellion corporate systems are isolated from all FTA systems, including those FTA systems of customers with Accellion-arranged hosting. Neither the FTA software nor FTA customer data is hosted on Accellion's corporate network.

Who was responsible for the attack activity? Was it a state-sponsored actor?

Accellion has no direct knowledge of who is responsible, but Mandiant is tracking the criminal organizations responsible for the data theft from FTA systems as UNC2546, and for subsequent extortion activity as UNC2582. For more information, please see Mandiant's recent blog post: Cyber Criminals Exploit Accellion FTA.

Is law enforcement investigating this incident?

Yes. The FBI has opened an investigation with which we have been fully cooperating.

Customer Impact and Support

How do I know if my FTA system was affected?

Accellion has identified the specific vectors, methods, and signatures of the FTA exploits, which have been confirmed by Mandiant. Detailed information is provided in the Mandiant report on the incident. Following this incident, Accellion developed a special tool for its clients to use on their systems to check for indicators of compromise associated with the exploit activity and to identify any files downloaded, if the system was exploited. We are available to help clients use this tool, so that they can determine what information was accessed or stolen in the event they were affected, but we have no ability to access the content of the information ourselves. We also continue to urge all FTA customers to upgrade to our flagship Kiteworks® content firewall platform as soon as possible.

Customer Impact and Support continued

What information was accessed or stolen?

By design, Accellion has no access to the content of data stored on a customer's FTA system. Each system is encrypted with keys available only to the client. To the extent Accellion has helped affected customers identify files downloaded from their FTA system, information about the downloaded files remains strictly customer-confidential.

Should we be notifying our customers?

Accellion does not have access to the encrypted data on any FTA system. However, as explained above, we can help you determine whether your system was compromised and if so what if any files were taken. Ultimately, the decision to make a notification must be made by you. It depends on the forensic analysis of your specific FTA system, your understanding of your data, and your legal, regulatory, and contractual requirements.

How are you supporting potentially affected FTA customers?

Accellion expediently issued patches for the relevant vulnerabilities as they were discovered and notified clients to update their systems immediately. We are now supporting clients in their forensic analysis to understand whether and how they were affected. In addition, we will no longer be renewing FTA licenses for customers beginning in April 2021 and are migrating FTA clients as rapidly as possible to the Kiteworks® content firewall platform, at no charge.

How are you supporting the broader cybersecurity community, so that other organizations can defend against similar exploits?

Accellion reported all vulnerabilities identified to the public Common Vulnerabilities and Exposures database. We have also conducted multiple confidential briefings with cybersecurity information sharing groups under the Department of Homeland Security Traffic Light Protocol and assisted in the issuance of a CISA advisory. Accellion has also worked closely with Mandiant to ensure the public disclosure of confirmed details of the incident, including in the report issued by Mandiant on the incident.

Accellion Product Security

Why should I trust the Kiteworks® platform? How is its security different from FTA?

The Kiteworks® content firewall platform was unaffected by these attacks. It is built on a completely different codebase, using state-of-the-art security architecture and devops security processes. Kiteworks® software is updated on an agile quarterly release cycle, undergoes extensive penetration testing on a regular basis, and has FedRAMP-compliant hosting options. While no system is immune from the threats posed by today's sophisticated criminal and nation-state hacking organizations, the Kiteworks® content firewall is designed and developed to provide the strongest defense available in the industry for sensitive third-party communications.

Are you providing any resources or discounts to affected customers?

All FTA customers can upgrade to the Kiteworks® content firewall free of charge. The Accellion "like for like" upgrade program allows FTA customers to upgrade at the same price to an equivalent Kiteworks® license, and the migration can be completed in less than week in most cases. In addition, the Kiteworks® platform comes with numerous built-in capabilities not available in FTA, at no additional cost, including plugins for Microsoft Outlook, Microsoft Office, and Google G-Suite that make sending secure files fast and easy, a secure mobile application, more advanced security and governance controls, a Splunk app, and a detailed syslog audit trail that is consolidated across all communication channels for incident detection, response, forensics and compliance. Accellion has already proactively upgraded its hosted FTA clients to the Kiteworks® platform.

Can I migrate to another system other than the Kiteworks® platform?

Yes. FTA customers can download content from their FTA system, which they can then move to any system of their choosing. However, the Kiteworks® content firewall is architected, developed, and delivered using state-of-the-art security practices and offers the highest level of protection available. In addition, we have specific tools built to help customers migrate from FTA to Kiteworks® quickly and efficiently.

What are you doing to enhance security going forward?

The Kiteworks® platform has a modern code base, development process, design, architecture, and security implementation. A strong team of engineers and architects, many with longstanding careers in cybersecurity, designed and built the Kiteworks® code base. The Kiteworks® development process leverages secure coding practices that align with ASVS OWASP guidelines. All Kiteworks® builds undergo rigorous internal white box testing and external testing through security bounty programs with competitive payout levels. Kiteworks® offers the highest strategic value to our clients and we continue to invest heavily in maintaining and improving its security.