FIREEYE™

ACCELLION, INC.

FILE TRANSFER APPLIANCE (FTA) SECURITY ASSESSMENT

MARCH 1, 2021

CONTENTS

Executive Summary

Mandiant was engaged by Accellion, Inc. (Accellion) to perform a security assessment of Accellion's File Transfer Appliance (FTA) software, in the wake of two related but distinct exploits used to attack client Accellion FTA systems—one that was discovered and addressed by Accellion in December 2020 (the "December Exploit"), and another that was discovered and addressed by Accellion in January 2021 (the "January Exploit") (collectively, the "Exploits").

The objectives of Mandiant's security assessment included:

- Independently identifying the security vulnerabilities used in the attack activity, based on review of compromised Accellion FTA instances
- Validating the patches that Accellion issued for the vulnerabilities
- Testing FTA version 9.12.432 (current as of the time of Mandiant testing) for further vulnerabilities in the software

This assessment was performed between February 4, 2021 and February 26, 2021.

Summary of Results

Accellion identified two zero-day vulnerabilities that were part of the December Exploit—CVE-2021-27101 and CVE-2021-27104—and two zero-day vulnerabilities that were part of the January Exploit—CVE-2021-27102 and CVE-2021-27103. Based on Mandiant's own forensic analysis of a sample of compromised Accellion FTA instances—which were provided to Mandiant by Accellion as well as impacted Accellion customers (in investigations Mandiant conducted directly for those customers), Mandiant confirmed that the attacker activity exploited these vulnerabilities (the "Exploited Vulnerabilities"). Mandiant did not identify any additional vulnerabilities that were exploited by the attackers.[1] Mandiant also validated the efficacy of the patches Accellion released to address the Exploited Vulnerabilities, which Accellion made available to FTA customers soon after each Exploit was identified.

The Exploited Vulnerabilities were of critical severity because they were subject to exploitation via unauthenticated remote code execution. Through its source code analysis and penetration testing, Mandiant did not identify any new such unauthenticated remote code-execution vulnerabilities. Mandiant did identify two previously unknown authenticated-user vulnerabilities: (1) Argument Injection (CVE-2021-27730), accessible to authenticated users with administrative privileges; and (2) Stored Cross-Site Scripting (CVE-2021-27731), accessible to regular authenticated users. The Argument Injection finding yielded a Common Vulnerability Scoring System (CVSS v3.0) score of 6.6 (medium severity) and the Stored Cross-Site Scripting finding was rated 8.1 (high severity). Accellion has developed a patch for these two vulnerabilities (FTA 9.12.444), which Mandiant has validated.

Project Scope

Accellion FTA Vulnerability Identification: Mandiant reviewed the source code for Accellion FTA versions 9.12.370 through 9.12.432, as well as a sample of ten (10) forensic images from affected Accellion FTA instances, in order to identify the vulnerabilities involved in the attack activity and to test for additional vulnerabilities. This review involved the following methods:

[1] As explained in a separate blog post, Mandiant has attributed the attack activity on FTA systems to two uncategorized threat groups—one that is believed to be responsible for compromising the systems (UNC2546), and another that is believed to be responsible for engaging in extortion activity with respect to a subset of the compromised customers (UNC2582).

1. Source code analysis
2. Dynamic penetration testing of Accellion FTA
3. Forensic analysis of compromised Accellion FTA appliances

Accellion FTA Patch Validation: Mandiant reviewed the Accellion FTA product version 9.12.432 (current as of the time of Mandiant's review) to validate that the version mitigated the Exploited Vulnerabilities. Mandiant then attempted variations of exploits to determine if the 9.12.432 version of Accellion FTA could be exploited using variations of the known attack vectors. The following areas were reviewed during this portion of the assessment:

1. Attempting alternative variations of the previously identified exploits
2. Attempting to exploit web pages and web services application programming interfaces (SOAP APIs) not used by attackers

Technical Details

This section describes the scope and technical details for this assessment.

Timeline of Events

Below is a timeline of the relevant events, starting with the first detection of anomalous activity, up to the latest Accellion FTA patch pushed to customers.

December Exploit	**Exploit**	•	Dec. 16, 2020:	First known use of December Exploit: exploit trips FTA's built-in anomaly detector on customer's device
	Investigation	•	Dec. 16, 2020:	Customer notifies Accellion that its anomaly detector was triggered
	Investigation	•	Dec. 16-19, 2020:	Accellion investigates and identifies vulnerabilities affecting FTA 9.12.370 – SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104)
	Mitigation	•	Dec. 20, 2020:	Accellion releases patch FTA 9.12.380, which remediates CVE-2021-27101 and CVE-2021-27104
	Mitigation	•	Dec. 23, 2020:	Accellion releases patch FTA 9.12.411, increasing anomaly detector checks from one per day to one per hour
January Exploit	**Exploit**	•	Jan. 20, 2021:	First known use of January Exploit (unknown to Accellion at the time)
	Exploit	•	Jan. 22, 2021:	Through multiple customer service inquiries, Accellion learns of anomalous activity indicative of new exploit
	Mitigation	•	Jan. 22, 2021:	Accellion issues critical security alert advising FTA customers to shut down their FTA systems immediately
	Mitigation	•	Jan. 22-25, 2021:	Accellion investigates and identifies Server-Side Request Forgery (CVE-2021-27103) and OS Command Execution (CVE-2021-27102) vulnerabilities
	Mitigation	•	Jan. 25, 2021:	Accellion releases patch FTA 9.12.416, which remediates CVE-2021-27102 and CVE-2021-27103
	Mitigation	•	Jan. 28, 2021:	Accellion releases patch FTA_9.12.432, increasing frequency of anomaly detector checks to every 10 minutes
Mandiant Review	**Review**	•	Feb. 4, 2021:	Mandiant begins security assessment
	Review	•	Feb. 28, 2021:	Mandiant concludes assessment, identifying two new findings – Argument Injection (CVE-2021-27730) and Stored XSS (CVE-2021-27731)
	Mitigation	•	Mar. 1, 2021:	Accellion releases patch FTA 9.12.444, addressing CVE-2021-27730 and CVE-2021-27731

Forensic Analysis

Materials Reviewed

In analyzing the Exploited Vulnerabilities previously identified by Accellion – SQL Injection (CVE-2021-27101), Server-Side Request Forgery (SSRF) (CVE-2021-27103), and OS Command Execution (CVE-2021-27102, CVE-2021-27104) – Mandiant had access to and reviewed forensic images from ten (10) affected Accellion FTA instances. The majority of the instances reflected activity associated with the December Exploit, while the others reflected activity associated with the January Exploit. Based on Mandiant's experience, the activity observed on these instances is likely to be representative of attacker activity on other affected instances not reviewed by Mandiant, given the repetitive, script-like execution of the activity observed. In some cases, in addition to the FTA instances themselves, Mandiant had access to firewall logs from the networks the FTA appliances were hosted on, which allowed Mandiant to identify additional evidence of attacker activity based on known attacker IP addresses.

How the Attack Operated

December Exploit

With respect to the December Exploit, Mandiant observed that the attacker chained together the following vulnerabilities: SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104). The attacker leveraged the SQL Injection vulnerability against the file `document_root.html` to retrieve "`W`" keys from the Accellion FTA database. These keys were then used to generate valid tokens that allowed the attacker to then make additional requests to a file named `sftp_account_edit.php`. While abusing the OS Command Execution vulnerability in this file, the attackers were able to execute their own commands, resulting in the creation of a web shell[2] written to `/home/seos/courier/oauth.api`.

The attacker likely used the newly created `oauth.api` web shell to upload a custom, more full-fledged web shell with the filename of `about.html` (variant 1) to disk, which included highly customized tooling designed to facilitate exfiltration of data from the FTA system. While the timing of the requests resulting in the generation of this second web shell suggests that it was delivered via the `oauth.api` web shell, the available evidence does not indicate the exact mechanism used to write it to disk. For threat-tracking purposes, Mandiant has labeled this second web shell as "DEWMODE".

The DEWMODE web shell extracts a list of available files from a MySQL database on the targeted Accellion FTA system and lists those files and corresponding metadata (file ID, path, filename, uploader, and recipient) on an HTML page. File download requests are captured in the web logs for the Accellion FTA system, which will contain requests to the DEWMODE web shell with encrypted and encoded URL parameters, where `dwn` is the file path and `fn` is the requested file name. The DEWMODE webshell has features that allow the attacker to delete the Accellion FTA web logs. Forensic analysts may need to recover these logs from slack space for analysis.

The uploading of the DEWMODE web shell to the file location where the attacker placed it had the effect (likely unanticipated by and unknown to the attacker) of tripping the built-in anomaly detector included in the FTA software. Once the anomaly detector is tripped, it generates an email alert to the customer (specifically to the admin email account designated by the customer), advising the customer to contact Accellion for support. As a result, any FTA customer affected by the December Exploit likely was sent such an email – which, per Accellion, is how the December Exploit came to its attention (see above Timeline).

[2] A web shell is a script that can be uploaded to a web server to enable remote execution of commands.

January Exploit

Mandiant observed that, after the December 20, 2020 release of patch 9.12.380, which remediated the vulnerabilities associated with the December Exploit, the attacker pivoted to a new technique involving Server-Side Request Forgery (SSRF) (CVE-2021-27103) and OS Command Execution (CVE-2021-27102).

The attacker chained together an SSRF vulnerability (CVE-2021-27103) with a Command Execution vulnerability (CVE-2021-27102) to execute commands on the system. Specifically, the attacker leveraged the SSRF vulnerability against the file `wmProgressstat.html` to reach a local SOAP web service located in the file `sw_update.php`, which would not otherwise be accessible from the Internet. Once access was established with the file `sw_update.php`, the attacker abused the OS Command Execution vulnerability in this file to create other malicious files, including another `about.html` (variant 2) DEWMODE web shell used to further the remainder of their attack.

Notably, in the case of this second exploit, the attacker uploaded the DEWMODE web shell to a different location (`/home/httpd/html/about.html`), likely to avoid FTA's built-in anomaly detector. The earliest evidence we have seen of this change in tactic appears on January 20, 2020.

Both Exploits

Both the December Exploit and the January Exploit demonstrate a high level of sophistication and deep familiarity with the inner workings of the Accellion FTA software, likely obtained through extensive reverse engineering of the software. Among the things the attacker had to know were:

- How to call internal APIs to obtain keys to decrypt filenames
- How to forge tokens for internal API calls
- How to chain together the vulnerabilities involved to conduct unauthenticated remote code execution
- How to navigate FTA's internal database, requiring a detailed understanding of the database structure
- How to bypass FTA's built-in anomaly detector (in the case of the January Exploit)

Indicators of Compromise

Based on Mandiant's review of the logs and images available for analysis, the attacker activity generated the following signatures for each affected customer, all of which should be considered as signs of potential compromise:

December Exploit

The December Exploit, which leveraged SQL Injection (CVE-2021-27101) and OS Command Execution (CVE-2021-27104), yielded Indicators of Compromise (IOCs) of the following files with their respective directories:

- `/home/seos/courier/about.html` (DEWMODE)
- `/home/seos/courier/httpd.pid`
- `/home/seos/courier/oauth.api`
- `/home/seos/courier/DF`
- `/tmp/.out`
- `/tmp/.scr`
- `/home/seos/courier/cache.jz.gz`

As noted above, the attacker activity tripped FTA's anomaly detector, causing an alert to be sent to the administrator of the affected customer's application.

During the cleanup routine, the attacker passed a specific query parameter named `csrftoken` with the value `11454bd782bb41db213d415e10a0fb3c` to DEWMODE. This would cause the following actions:

- A shell script is written to `/tmp/.scr`, which will:

    - Remove all references to about.html from log files located in `/var/opt/apache/`
    - Write the modified log file to `/tmp/x` then attempt to replace the original log file at `/var/opt/apache/`
    - Delete the contents of the `/home/seos/log/adminpl.log` log file
    - Remove `/home/seos/courier/about.html` (DEWMODE) and `/home/seos/courier/oauth.api` (eval web shell), and redirect command output to the file `/tmp/.out`
    - Change the permissions of the output file to be readable, writeable and executable by all users, and set the owner to "nobody"
- Delete the script file `/tmp/.scr` and other temporarily created files to assist in cleanup
- Display cleanup output to the requesting user

January Exploit

The January Exploit, which leveraged Server-Side Request Forgery (SSRF) (CVE-2021-27102) and OS Command Execution (CVE-2021-27103), yielded IOCs of the following files with their respective directories:

- `/home/httpd/html/about.html` (DEWMODE)
- `/home/httpd/html/httpd.pid`
- `/home/httpd/html/oauth.api`
- `/home/httpd/html/DF`
- `/tmp/.out`
- `/tmp/.scr`
- `/home/httpd/html/cache.jz.gz`

The variant instance of DEWMODE used in the January Exploit (`bdfd11b1b092b7c61ce5f02ffc5ad55a`) had a slightly modified cleanup routine, which included wiping of `/var/log/secure` and removing `about.html` and `oauth.api` from the directories `/home/httpd/html/` instead of `/home/seos/courier/`.

During the cleanup routine, the attacker removed all references of the `about.html` webshell from systems' `/var/opt/apache` log files, cleared the `/home/seos/log/adminpl.log` file, removed files from the `/home/httpd/html` directory, and cleared the `/var/log/secure` log file. This variant of `about.html` and the anti-forensic script appear to be an improvement of the earlier variant of `about.html`, which failed to clear the `/var/log/secure` log file where previous versions of the anti-forensic script were recorded. Mandiant did identify evidence of the anti-forensic script execution within rolled versions of the `/var/log/secure` log file.

Validation of Accellion's Remediation of the Exploited Vulnerabilities

As reflected in the Timeline section, Accellion issued a patch addressing the vulnerabilities associated with the December Exploit on December 20, 2020 (four days after it started investigating anomalous activity associated with the exploit), and a patch addressing the vulnerabilities associated with the January Exploit on January 25, 2021 (three days after it started investigating anomalous activity associated with the exploit, having advised all FTA customers to shut down their FTA instances in the interim).

Accellion asked Mandiant to confirm that the patches successfully closed these Exploited Vulnerabilities, and that no other vulnerabilities were exploited as part of the attack activity. Mandiant's analysis confirmed both points.

Mandiant performed patch validation of Accellion FTA 9.12.432 (which includes the December 20 and January 22 patches) to validate that the latest version of Accellion FTA mitigates each of the four Exploited Vulnerabilities. As

part of this review, Mandiant reviewed the source code in both versions 9.12.370 (pre-dating both the December 20 and January 22 patches) and 9.12.432 to confirm that the changes completely mitigated the Exploited Vulnerabilities.

Mandiant also tested variations of the exploit techniques involved in the Exploits to ensure that Accellion's implementation of input validation and sanitization could not be bypassed. This component of the assessment included attempting alternative variations of the Exploits, as well as attempting to exploit web pages and SOAP APIs not initially used by attackers.

Based on these analyses, Mandiant confirmed that the patches issued by Accellion fully resolved the Exploited Vulnerabilities, as shown in the table below.

Identified Exploits	CVE	Affected Scope	Status
SQL Injection	CVE-2021-27101	document_root.html	Remediated
Command Injection	CVE-2021-27104	Multiple administrative API endpoints[3]	Remediated
Server-Side Request Forgery	CVE-2021-27103	wmProgressstat.html	Remediated
Command Injection	CVE-2021-27102	sw_update.php	Remediated

Mandiant also confirmed through forensic analysis of compromised Accellion FTA instances that the only vulnerabilities exploited in the attacker activity on the devices were the Exploited Vulnerabilities. Mandiant did not identify additional vulnerabilities that were part of the attacker activity.

Testing FTA for Additional Vulnerabilities

Objectives and Methodology

Accellion also asked Mandiant to review the Accellion FTA software for any other vulnerabilities Mandiant was able to find, beyond the Exploited Vulnerabilities. Specifically, Mandiant reviewed the versions of the software dating from December 16, 2020 to the time of Mandiant's review, including:

- 9.12.370
- 9.12.380
- 9.12.411
- 9.12.416
- 9.12.432

Mandiant's review relied on both source code analysis and dynamic penetration testing:

- Source code analysis: Mandiant was provided a copy of unobfuscated source code by Accellion. Mandiant was also provided a list of unauthenticated endpoints provided by Accellion to prioritize. Mandiant reviewed the source code using manual techniques and did not rely on automated source code review tools.

[3] An API endpoint can be a URL of a webpage or web service.

- Dynamic penetration testing: The focus of the dynamic penetration testing phase of the assessment was to identify vulnerabilities by directly interacting with the Accellion FTA software. To facilitate this testing, Mandiant primarily used Burp Suite Professional ("Burp Suite"), a multifunction web proxy. Mandiant began the assessment by prioritizing analysis of endpoints that did not require authentication.

Mandiant began to review the files corresponding to endpoints, looking for insecure usage of functions that accept input from an untrusted source. This methodology is referred to as "taint analysis," as it involves identifying potentially insecure functions where an untrusted user input is being supplied. Mandiant analyzed each result from such inputs to determine if any vulnerabilities were surfaced. As a result of this analysis, Mandiant identified a Stored XSS vulnerability (CVE-2021-27731) resulting from lack of input validation or sanitization.

Mandiant continued this analysis by manually searching for sensitive or insecure PHP built-in functions that accepted untrusted input. Mandiant searched for insecure functions by referencing various documentation on the Internet detailing functions which have been historically exploited. In addition, Mandiant searched for additional instances of the functions exploited as part of the Exploited Vulnerabilities, to ensure untrusted inputs were not being provided to these functions. As a result of Mandiant's analysis of application endpoints accessible only to an administrator, Mandiant observed application endpoints calling a local Perl script named `admin.pl`. Specifically, Mandiant searched for usage of the insecure PHP functions `escapeshellargs` and `escapeshellcmd` used in conjunction with this function. After triaging the output, Mandiant identified a single API endpoint that did not properly sanitize user input, allowing Mandiant to inject an argument when calling the `admin.pl` script (CVE2021-27730).

Mandiant then proceeded to review the source code of each file corresponding to application API endpoints. This was necessary as the majority of these application endpoints were not accessible from the application user interface. In instances where functionality potentially of use to an attacker was identified, Mandiant attempted to craft requests and manipulate inputs to probe for vulnerabilities and observe the application's behavior. Specifically, Mandiant searched for functionality potentially susceptible to injection-based issues allowing for remote code execution or unauthorized access to data stored within the SQL database or on the remote file system. Mandiant did not identify any vulnerabilities as a result of this analysis.

Mandiant also carefully evaluated the Accellion FTA software's authentication logic to ensure it was not vulnerable to an authentication bypass issue, which might allow an attacker to access an authenticated endpoint without being validly authenticated. In addition to searching for injection-based issues, Mandiant searched for issues which could allow for users to bypass authentication or authorization controls. For example, Mandiant attempted to tamper with inputs containing session information such as cookies or tokens, to see if the requested application endpoint or file could still be accessed. Mandiant did not identify any vulnerability through this analysis.

Results of Testing FTA for Additional Vulnerabilities

The Exploited Vulnerabilities were of critical severity because they allowed for remote code execution by an unauthenticated user. Mandiant's source code analysis and penetration testing did not identify any new unauthenticated remote code-execution vulnerabilities beyond the Exploited Vulnerabilities.

Mandiant identified two new findings for *authenticated* users, consisting of Argument Injection (CVE-2021-27730), which was accessible only to authenticated users with administrative privileges, and a Stored Cross-Site Scripting (CVE-2021-27731), which was accessible only to regular authenticated users. The Argument Injection finding yielded a CVSS v3.0 score of 6.6 (medium severity) and the Stored Cross-Site Scripting finding was rated 8.1 (high severity).

After being alerted to Mandiant's findings, Accellion developed FTA patch 9.12.444 to address these newly identified findings. Mandiant validated that the patch effectively remediated these vulnerabilities, specifically attempting to exploit FTA version 9.12.444 and confirming that injected input was correctly sanitized.

Disclaimer: While every precaution has been taken in the preparation of this document, neither Accellion nor Mandiant assumes any responsibility for errors or omissions resulting from the use of the information herein.

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent, and respond to cyber attacks. FireEye has over 5,300 customers across 67 countries, including more than 845 of the Forbes Global 2000.