Exploitation of Accellion File Transfer Appliance

us-cert.cisa.gov/ncas/alerts/aa21-055a

Summary

This joint advisory is the result of a collaborative effort by the cybersecurity authorities of Australia,[1] New Zealand,[2] Singapore,[3] the United Kingdom,[4] and the United States.[5] [6] These authorities are aware of cyber actors exploiting vulnerabilities in Accellion File Transfer Appliance (FTA).[7] This activity has impacted organizations globally, including those in Australia, New Zealand, Singapore, the United Kingdom, and the United States.

Worldwide, actors have exploited the vulnerabilities to attack multiple federal and state, local, tribal, and territorial (SLTT) government organizations as well as private industry organizations including those in the medical, legal, telecommunications, finance, and energy sectors. According to Accellion, this activity involves attackers leveraging four vulnerabilities to target FTA customers.[8] In one incident, an attack on an SLTT organization potentially included the breach of confidential organizational data. In some instances observed, the attacker has subsequently extorted money from victim organizations to prevent public release of information exfiltrated from the Accellion appliance.

This Joint Cybersecurity Advisory provides indicators of compromise (IOCs) and recommended mitigations for this malicious activity. For a downloadable copy of IOCs, see: AA21-055B.stix and MAR-10325064-1.v1.stix.

Click herefor a PDF version of this report.

Technical Details

Accellion FTA is a file transfer application that is used to share files. In mid-December 2020, Accellion was made aware of a zero-day vulnerability in Accellion FTA and released a patch on December 23, 2020. Since then, Accellion has identified cyber actors targeting FTA customers by leveraging the following additional vulnerabilities.

- CVE-2021-27101 – Structured Query Language (SQL) injection via a crafted HOST header (affects FTA 9_12_370 and earlier)
- CVE-2021-27102 – Operating system command execution via a local web service call (affects FTA versions 9_12_411 and earlier)
- CVE-2021-27103 – Server-side request forgery via a crafted POST request (affects FTA 9_12_411 and earlier)
- CVE-2021-27104 – Operating system command execution via a crafted POST request (affects FTA 9_12_370 and earlier)

One of the exploited vulnerabilities (CVE-2021-27101) is an SQL injection vulnerability that allows an unauthenticated user to run remote commands on targeted devices. Actors have exploited this vulnerability to deploy a webshell on compromised systems. The webshell is located on the target system in the file `/home/httpd/html/about.html` or `/home/seos/courier/about.html`. The webshell allows the attacker to send commands to targeted devices, exfiltrate data, and clean up logs. The clean-up functionality of the webshell helps evade detection and analysis during post incident response. The Apache `/var/opt/cache/rewrite.log` file may also contain the following evidence of compromise:

- `[.'))union(select(c_value)from(t_global)where(t_global.c_param)=('w1'))] (1) pass through /courier/document_root.html`
- `[.'))union(select(reverse(c_value))from(t_global)where(t_global.c_param)=('w1'))] (1) pass through /courier/document_root.html`
- `['))union(select(loc_id)from(net1.servers)where(proximity)=(0))] (1) pass through /courier/document_root.html`

These entries are followed shortly by a pass-through request to `sftp_account_edit.php`. The entries are the SQL injection attempt indicating an attempt at exploitation of the HTTP header parameter `HTTP_HOST`.

Apache access logging shows successful file listings and file exfiltration:

- `“GET /courier/about.html?aid=1000 HTTP/1.1” 200 {Response size}`
- `“GET /courier/about.htmldwn={Encrypted Path}&fn={encrypted file name} HTTP/1.1” 200 {Response size}`

When the clean-up function is run, it modifies archived Apache access logs `/var/opt/apache/c1s1-access_log.*.gz` and replaces the file contents with the following string:

```
Binary file (standard input) matches
```

In two incidents, the Cybersecurity and Infrastructure Security Agency (CISA) observed a large amount of data transferred over port 443 from federal agency IP addresses to `194.88.104[.]24`. In one incident, the Cyber Security Agency of Singapore observed multiple TCP sessions with IP address `45.135.229[.]179`.

Organizations are encouraged to investigate the IOCs outlined in this advisory and in AR21-055A. If an Accellion FTA appears compromised, organizations can get an indication of the exfiltrated files by obtaining a list of file-last-accessed events for the target files of the symlinks located in the `/home/seos/apps/1000/` folder over the period of malicious activity. This information is only indicative and may not be a comprehensive identifier of all exfiltrated files.

Mitigations

Organizations with Accellion FTA should:

- Temporarily isolate or block internet access to and from systems hosting the software.
- Assess the system for evidence of malicious activity including the IOCs, and obtain a snapshot or forensic disk image of the system for subsequent investigation.
- If malicious activity is identified, obtain a snapshot or forensic disk image of the system for subsequent investigation, then:
    - Consider conducting an audit of Accellion FTA user accounts for any unauthorized changes, and consider resetting user passwords.
    - Reset any security tokens on the system, including the “W1” encryption token, which may have been exposed through SQL injection.
- Update Accellion FTA to version FTA_9_12_432 or later.
- Evaluate potential solutions for migration to a supported file-sharing platform after completing appropriate testing.

    Accellion has announced that FTA will reach end-of-life (EOL) on April 30, 2021. [9] Replacing software and firmware/hardware before it reaches EOL significantly reduces risks and costs.

Additional general best practices include:

- Deploying automated software update tools to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
- Only using up-to-date and trusted third-party components for the software developed by the organization.
- Adding additional security controls to prevent the access from unauthenticated sources.

Resources

- FireEye Blog – 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
- Australia, Canada, New Zealand, the United Kingdom, and the United States Joint Advisory on Technical Approaches to Uncovering and Remediating Malicious Activity
    https://us-cert.cisa.gov/ncas/alerts/aa20-245a
- CISA and MS-ISAC’s Ransomware Guide
    https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

References

Revisions

February 24, 2021: Initial Version

June 17, 2021: Replaced STIX file to remove an IOC reported as non-malicious.

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.