Qualys Data Breach Review

On March 3, 2021, cybersecurity firm Qualys announced that threat actors had exploited zero-day vulnerabilities in their Accellion FTA server to steal data files, making it the latest victim in a string of attacks against Accellion customers that started in December.

Qualys received an integrity alert on December 24, 2020, confirming that unauthorized access was made to its clients' files. Data exposed on CL0p's leak site (CL0P^-LEAKS) included purchase orders, invoices, tax documents, and scan reports. Fewer than 100 of Qualys' customers were affected. The attack had no impact on Qualys' productions environments, codebase, or customer data hosted on the Qualys Cloud Platform. All its platforms remained full functional and there was no operational impact at any point.

Previous victims received ransom notes for their data via email, alerting them that their data had been exfiltrated and would be published unless they paid a ransom. However, it is unknown whether Qualys received one. Upon receiving the alert, Qualys immediately notified its affected customers, isolated the affected system from the network, and created an alternative process to support its customers' file transfer needs. That device (fts-na.qualys.com) has been decommissioned since then, and according to Shodan, was last active on February 19, 2021.

Qualys' vendor Accellion has brought on FireEye Mandiant to research the attacks on their FTA servers. Mandiant is tracking the exploitation of these vulnerabilities as UNC2546, and the extortion activity as UNC2582. Qualys has also asked Mandiant for assistance in the investigation on their own attacks.

The attackers, the CL0p ransomware gang working in conjunction with the FIN11 threat group, exploited multiple zero-day vulnerabilities in Accellion's legacy FTA (File Transfer Appliance) and a new web shell called DEWMODE to steal hosted files. While CL0p typically encrypts victim data, no CL0p file-encrypting malware or ransomware was deployed in the attack on Qualys. The exploit takes advantage of a SQL injection vulnerability that culminates in writing a custom web shell to the system. The web shell extracts a list of available files from a mySQL database on the FTA and lists them on an HTML page along with the metadata including file ID, path, filename, uploader and recipient.

At that time, Qualys used an Accellion FTA server in a DMZ, a subnet environment separate from untrusted networks, in particular the public internet. The server was used to facilitate the encrypted temporary transfer of manually uploaded files and was separate from the Qualys Cloud Platform. On December 21, 2020, Accellion published a hotfix to remedy vulnerabilities it had found in its 20-year-old legacy appliance. Qualys applied them on December 22, 2020, two days before it received the integrity alert.

Attacking third party providers provides access to their clients, who can then be held for ransom. Given the large number of customers third-party providers such as Accellion support, it is likely that attackers will continue to explore vulnerabilities in their products and accelerate their attacks against their customers. Yet, as a Forbes Global 100 information security provider with 10,000 clients in over 130 countries, Qualys is a highly valuable target in its own right. While ransom is profitable, access to the law firms', government bodies', and large corporations' unencrypted data could be leveraged not only for extortion but also to pursue additional victims.

As of April 30, 2021, Accellion does not support its FTA servers. It recommends all its customers migrate to its Kiteworks products which are unaffected by the vulnerabilities the attackers exploited. In addition to making proper backups of their data, organizations that transfer large files should consider encrypting them before transfer to protect them against exposure to unauthorized entities.

Vulnerability Details:

Mandiant identified four zero-day vulnerabilities in the process of investigating the Accellion attacks. Two were involved in the December attacks, including the ones against Qualys. Two other exploits were employed in January's attacks against other Mandiant clients.

CVE-2021-27101

Accellion FTA 9_12_370 and earlier is affected by SQL injection via a crafted Host header in a request to document_root.html. The fixed version is FTA_9_12_380 and later. It affects software versions up to and including 9_12_370.

CVE-2021-27102

Accellion FTA 9_12_411 and earlier is affected by OS command execution via a local web service call. The fixed version is FTA_9_12_416 and later. It affects software versions up to and versions 9_12_411.

CVE-2021-27103

Accellion FTA 9_12_411 and earlier is affected by SSRF via a crafted POST request to wmProgressstat.html. The fixed version is FTA_9_12_416 and later. It affects software versions up to and including 9_12_411.

CVE-2021-27104

Accellion FTA 9_12_370 and earlier is affected by OS command execution via a crafted POST request to various admin endpoints. The fixed version is FTA_9_12_380 and later. It affects software versions up to and including 9_12_370.

Source Material:

BleepingComputer. Cybersecurity firm Qualys is the latest victim of Accellion hacks. Published Mar 3, 2021.

TechTarget. Accellion FTA attacks claim more victims Published Mar 3, 2021.

Qualys. Qualys Update on Accellion FTA Security Incident. Published Mar 3, 2021. Updated Apr 2, 2021.

Computer Weekly. Qualys caught up in Accellion FTA breach Published Mar 4, 2021.

Computer Weekly. Oil giant Shell hit through Accellion FTA breach Published Mar 24, 2021.

TechTarget. Accellion breach raises notification concerns. Published Jun 14, 2021.

Background:

Accellion. Accellion Provides Update to Recent FTA Security Incident. Published Feb 1, 2021.

DataBreaches.net. Threat actors claim to have stolen Jones day files; law firm remains quiet. Published Feb 13, 2021.

Vice. Hacker Leaks Files from Jones Day Law Firm, Which Worked on Trump Election Challenges. Published Feb 16, 2021.

Computer Weekly. Law firm and cyber criminals clash over source of stolen data. Published Feb 17, 2021.

TechTarget. Wide net case on potential Accellion breach victims. Published Feb 17, 2021.

FireEye. Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion. Published Feb 22, 2021.

BleepingComputer. Global Accellion data breaches linked to Clop ransomware gang. Published Feb 22, 2021.

Accellion, Inc. File Transfer Appliance (FTA) Security Assessment. Published Mar 1, 2021.

Deutsche Telekom Security GmbH. Inside of CL0P's ransomware operation. Published Unknown Date.