ENPM686-0201

Samridha Murali

02/05/2022

Current Event 2

Towards the end of 2020 a cyber crime group identifies as UNC2546 target and attached Accellion File Transfer Application (FTA) server. The Accellion FTA device is a purpose built application designed to allow enterprise to securely transfer large files. UNC2446 explioted 4 zero-day vulnerabilities in Accellion's legacy FTA to install a newly discovered web shell called DEWMODE. Starting from late January 2022 several organizations that had impacted by UNC2546 in prior month began to receive emails from UNC2546 to publish stolen data on "CLOP^_-LEAKS".onion website.

Nearly 100 Accellion FTA clients were impacted, with affected organizations in mutiple sectors (finance, government, legal, education, telecommunications, healthcare and manufacturing) and multiple contries (the US, the UK, Australia, New Zealand, Singapore). Some major organizations that were affected by this are Bombardier(Canadian airplane manufacturer), Tansport of New South Wales(Australian government agency), Flagstar bank (one of the largest banks in the United States), Qualys (Cyber Security Company with revenue of 363 million), University of Colorando.

Deploy Automated software update tools to ensure that third party software on all the system is running the most recent security updates provided by software vendor. Accellion has released patches for all the vulnerabilities associated with this breach, and organizations using Accellion FTA server should update to their newest version. Suppose if a system is running Accellion FTA, system must be isolated from the internet until patches are released and applied. If malicious activity is identified CISA (Cybersecurity and Infrastructure Security Agency) recommends resetting the "W1" encryption token and any other security tokens on the system.

Refereces :

1. Insikt Group (2021, March 12) https://www.recordedfuture.com/dewmode-accellion-supply-chain-impact/
2. ANDREW MOORE, GENEVIEVE STARK, ISIF IBRAHIMA, VAN TA, KIMBERLY GOODY (FEB 22, 2021) https://www.mandiant.com/resources/accellion-fta-exploited-for-data-theft-and-extortion