FBI & NSA Cyber Threat Concerns for Industry Partners

Office of Housing sent this bulletin at 03/13/2024 09:33 AM EDT

FBI & NSA Cyber Threat Concerns for Industry Partners

Dear Owners and Operators,

The Office of Multifamily is sharing information as a service to you about **current cyber threats** against small businesses / offices, and organizations which could include Multifamily program participants and those they work with. Please circulate this information as widely as possible to the organizations you work with for awareness and mitigation actions available (recommended by FBI, CISA, and NSA).

FBI-APT28-Summary

The FBI published a Joint Cyber Security Advisory in partnership with NSA highlighting the activity of Russian state-sponsored cyber actor's (APT28) use of compromised Ubiquiti EdgeRouters to facilitate malicious cyber operations worldwide. Due to their user-friendly Linux-based OS and ease of use makes them popular with consumers and because of their popularity and widespread use it makes them a favorable target for malicious threat actors. EdgeRouters provide limited protections such as firewalls and **do not auto update firmware/software; they must be updated manually by the consumer. The lack of these features allows for undetected compromise of these devices and make remediation a manual process**.

As early as 2022, APT28 actors had utilized compromised EdgeRouters to facilitate covert cyber operations against governments, militaries, and organizations around the world. Targeted countries include the United States.

APT28 actors used the compromised devices to collect credentials, network traffic and have utilized them to host fraudulent landing pages and additional custom tools.

The FBI and their partners recommend factory resetting any compromised devices, updating to the latest firmware, changing any default credentials and implementing rules to limit administrative access from the internet on the devices.