THREAT BULLETINS

US Federal Agencies Issue New Recommendations for VSAT Communications

TLP:WHITE

Jan 28, 2022

The United States Federal Bureau of Investigation (FBI) and National Security Agency (NSA) have identified a potential increased risk to data transmitted by Very Small Aperture Terminals (VSAT). Given the rising geopolitical tensions, vulnerable VSAT implementations may be an attack vector for threat actors looking to gain sensitive visibility into unencrypted transmissions.

According to the agencies, network defenders should conduct an asset inventory of VSAT appliances within their environment to conduct further analysis of best practices given the newly released federal recommendations.

The FBI alert, which can be accessed here, and the NSA alert, which can be accessed here, are released at TLP:WHITE for community awareness. Health-ISAC members are encouraged to use the

intelligence and recommendations in this alert in conjunction with their own security posture.

VSAT networks are increasingly used for remote communications and utilize Transmission Control Protocol, Internet Protocol, and radio-frequency channels to transmit data. Due to the nature of VSAT network communication links and recent vulnerabilities discovered in VSAT terminals, network communications over these links are at risk of being exposed and may be targeted for the information they contain or to compromise connected networks.

Most of these links are unencrypted and rely on frequency separation or hopping to separate communications.

Recently conducted research discovered man-in-the-middle attacks against maritime VSAT signals can be conducted at low cost to threat actors, disabling a previous barrier and presenting opportunities for threat actors to potentially gain visibility into sensitive information.

Reference(s)	NSA, uscg, uscg, Defense

Recommendations
The National Security Agency (NSA) recommends that all organizations take an asset inventory and recognize if VSATs are in use by your organization. If they are:

- Ensure that VSATs are up to date with the most current patch applied from trusted, known-good sources.
- Ensure that default passwords are removed and changed.
- Ensure that VSAT networks are segmented.

In addition, the NSA's recommendations on encrypting network communications over VSAT links can be found here. As VSATs can be used as a backdoor to get into a network, these recommendations should be applied as quickly as possible.

Sources
National Security Agency – Protecting VSAT Communications

National Security Agency – NSA Issues Recommendations to Protect VSAT Communications

Federal Bureau of Investigation – Warning – VSAT Signals Vulnerable to Low-Cost Device Exploitation

Federal Bureau of Investigation - Private Industry Notification

Alert ID c54f1c92

View Alert

Tags Very Small Aperture Terminals, VSAT, NSA, FBI, Ukraine

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**