Protecting VSAT Communications

VSAT communications are at risk

Commercial Very Small Aperture Terminal (VSAT) networks are increasingly used for remote communications in support of U.S. government missions. 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 by adversaries for the sensitive information they contain or to compromise connected networks. Most of these links are unencrypted, relying on frequency separation or predictable frequency hopping rather than encryption to separate communications. Public vulnerability research has found certain terminal equipment vulnerable to compromise and illicit firmware modification [1]. NSA recommends that VSAT networks enable any available transmission security (TRANSEC) protections, segment and encrypt network communications before transmitting across the VSAT links, and keep VSAT equipment and firmware up to date.

NSA recommends:

- **Enabling TRANSEC**
- **Segmenting and encrypting networks before VSAT links**
- **Updating equipment and firmware**

Recent Russian cyber activity in Ukraine further underscores the risk to VSAT communications for both espionage and disruption. According to a recent U.S. and European Union statements, the Russian military launched cyber attacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the invasion, and those actions had spillover impacts into other European countries. The activity disabled very small aperture terminals in Ukraine and across Europe, including tens of thousands of terminals outside of Ukraine that, among other things, support wind turbines and provide Internet services to private citizens [2].

Encrypt network communications over VSAT links

VSAT systems (including terminals, modems, and ground stations) should be treated as unencrypted wireless networks for cybersecurity purposes. In other words, they should not be relied on to provide confidentiality from motivated cyber actors. Although they offer "virtual" network separation capabilities, such logical isolation cannot be trusted to

provide access control, separation, or confidentiality of sensitive information. Further, many of these networks can be gateways to the Internet, making them easy targets for remote exploitation. When using VSAT networks—as with any other untrusted transport network—information should first be secured using network encryption solutions to achieve confidentiality and protect against malicious cyber activity. According to US policy, controlled unclassified information (CUI) should be encrypted with commercial network encryption solutions, such as Internet Protocol Security (IPsec) or Transport Layer Security virtual private networks (TLS VPNs) first. Depending on network needs, many solutions exist to provide scalable encryption links.

Point-to-point communications over otherwise unencrypted IP-based networks may utilize (in accordance with NIST SP 800-131A rev2 and SP 800-56A rev3 guidance) IKE/IPsec-encrypted VPNs using certificates or pre-shared keys to authenticate peers and a Diffie-Hellman (DH) key exchange of at least 3072 bits or Elliptic Curve DH (ECDH) keys of 384 bits or larger (groups 14, 15, 16, 19, or 20) [3]. Point-to-point communications for National Security Systems should conform to CNSSP 15 standards [2]. Pre-shared keys should not be used with aggressive mode and should be protected from unauthorized disclosure. These IPsec VPNs provide mutual authentication to both ends of the VPN and protect the confidentiality of the data in transit. Similar cryptographic algorithms should be employed for TLS-based VPNs. Multipoint encrypted VPNs may be appropriate in architectures where many point-to-point VPNs are unmanageable. Examples of commercial multipoint VPN products include Cisco® GET VPN, Cisco FlexVPN (previously known as DMVPN), and Juniper® Auto Discovery VPN (ADVPN).

Encrypted VPN solutions protect the authenticity, integrity, and confidentiality of network traffic before passing it over the VSAT link. NSA recommends using mutually authenticated, encrypted TRANSEC. The encryption should be applied down to and including the outermost vendor-proprietary transmission protocol, using an NSA-approved cryptographically generated pseudorandom key stream (AES 256) and key management scheme.

Best practice guidance on using commercial satellite communications (SATCOM) is that network owners not use descriptive naming conventions and identifiers in SATCOM and mobile communications device configurations. This can complicate identification of devices and network topologies by external actors to understand their purposes.

Additional VSAT best practices

NSA recommends keeping all IT equipment up to date. VSAT equipment is no exception [4]. Networking equipment is increasingly becoming a target for malware, and the vulnerabilities above suggest that VSAT terminals and network infrastructure could be targeted like other networking technologies. Avoiding direct Internet access can reduce the attack surface, but should not be seen as a substitute for closing known terminal equipment vulnerabilities through software and firmware updates. Device updates and upgrades should be acquired from trusted, known-good sources.

In addition, VSAT systems utilize vendor-specific default credentials, which are published in user manuals; these passwords can enable root access to VSAT network management systems. NSA recommends changing all default credentials.

VSAT networks are designed for high-availability connections with sometimes little in terms of default authentication measures. Due to this, NSA recommends that VSAT networks be segmented with approved firewalls and other similar technology. This segmentation should isolate the management plane of the network, such as the network management system, so that it is not accessible by remote VSAT modems apart from vendor-identified ports and protocols.

Worldwide connectivity

Commercial VSAT technologies provide valuable, worldwide connectivity options, enabling multiple mission types when more robust options are unavailable or impractical. Users of such networks should ensure that data transmissions are encrypted, adopt network hygiene best practices, and seek to continuously monitor the VSAT network for unauthorized activity. Users should consider possible threats and the associated mission impacts when selecting SATCOM solutions.▪

Works cited

[1] R. Santamarta, Lecture and White Paper, BlackHat USA (2018), Topic: “Last Call for SATCOM Security,” Available at: https://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf

[2] State Department (2022), State Department Attribution Statement Press Release. Available at: https://www.state.gov/press-releases/

[3] Committee on National Security Systems (2016), CNSSP 15 Use of Public Standards for Secure Information Sharing. Available at: http://www.cnss.gov/CNSS/issuances/Policies.cfm

[4] National Security Agency (2019), Update and Upgrade Software Immediately. Available at: https://www.nsa.gov/cybersecurity-guidance

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Cisco is a registered trademark of Cisco Technology, Inc. • Juniper is a registered trademark of Juniper Networks, Inc.

Purpose

This document was developed in furtherance of NSA’s cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov

Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov