Alert (AA22-076A)

More Alerts

Strengthening Cybersecurity of SATCOM Network Providers and Customers

Original release date: March 17, 2022 | Last revised: May 10, 2022

Summary

Updated May 10, 2022: The U.S. government attributes this threat activity to Russian state-sponsored malicious cyber actors. Additional information may be found in a statement from the State Department. For more information on Russian malicious cyber activity, refer to cisa.gov/uscert/russia.

Actions to Take Today:
- Use secure methods for authentication.
- Enforce principle of least privilege.
- Review trust relationships.
- Implement encryption.
- Ensure robust patching and system configuration audits.
- Monitor logs for suspicious activity.
- Ensure incident response, resilience, and continuity of operations plans are in place.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) are aware of possible threats to U.S. and international satellite communication (SATCOM) networks. Successful intrusions into SATCOM networks could create risk in SATCOM network providers' customer environments.

Given the current geopolitical situation, CISA's Shields Up initiative requests that all organizations significantly lower their threshold for reporting and sharing indications of malicious cyber activity. To that end, CISA and FBI will update this joint Cybersecurity Advisory (CSA) as new information becomes available so that SATCOM providers and their customers can take additional mitigation steps pertinent to their environments.

CISA and FBI strongly encourages critical infrastructure organizations and other organizations that are either SATCOM network providers or customers to review and implement the mitigations outlined in this CSA to strengthen SATCOM network

cybersecurity.

Click here for a PDF version of this report.

Mitigations

CISA and FBI strongly encourages critical infrastructure organizations and other organizations that are either SATCOM network providers or customers to review and implement the following mitigations:

Mitigations for SATCOM Network Providers

- Put in place **additional monitoring at ingress and egress points** to SATCOM equipment to look for anomalous traffic, such as:
  - The presence of insecure remote access tools—such as Teletype Network Protocol (Telnet), File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Secure Copy Protocol (SCP), and Virtual Network Computing (VNC)—facilitating communications to and from SATCOM terminals.
  - Network traffic from SATCOM networks to other unexpected network segments.
  - Unauthorized use of local or backup accounts within SATCOM networks.
  - Unexpected SATCOM terminal to SATCOM terminal traffic.
  - Network traffic from the internet to closed group SATCOM networks.
  - Brute force login attempts over SATCOM network segments.
- See the Office of the Director of National Intelligence (ODNI) Annual Threat Assessment of the U.S. Intelligence Community, February 2022 for specific state-sponsored cyber threat activity relating to SATCOM networks.

Mitigations for SATCOM Network Providers and Customers

- **Use secure methods for authentication,** including multifactor authentication where possible, for all accounts used to access, manage, and/or administer SATCOM networks.
  - Use and enforce strong, complex passwords: Review password policies to ensure they align with the latest NIST guidelines.
  - **Do not use default credentials or weak passwords.**
  - Audit accounts and credentials: remove terminated or unnecessary accounts; change expired credentials.
- **Enforce principle of least privilege through authorization policies.** Minimize unnecessary privileges for identities. Consider privileges assigned to individual personnel accounts, as well as those assigned to non-personnel accounts (e.g., those assigned to software or systems). Account privileges should be clearly defined, narrowly scoped, and regularly audited against usage patterns.
- **Review trust relationships.** Review existing trust relationships with IT service providers. Threat actors are known to exploit trust relationships between providers and their customers to gain access to customer networks and data.
  - Remove unnecessary trust relationships.

    - Review contractual relationships with all service providers. Ensure contracts include appropriate provisions addressing security, such as those listed below, and that these provisions are appropriately leveraged:
        - Security controls the customer deems appropriate.
        - Provider should have in place appropriate monitoring and logging of provider-managed customer systems.
        - Customer should have in place appropriate monitoring of the service provider's presence, activities, and connections to the customer network.
        - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks.
- **Implement independent encryption** across all communications links leased from, or provided by, your SATCOM provider. See National Security Agency (NSA) Cybersecurity Advisory: Protecting VSAT Communications for guidance.
- Strengthen the security of **operating systems, software, and firmware.**
    - Ensure robust **vulnerability management and patching** practices are in place and, after testing, immediately patch known exploited vulnerabilities included in CISA's living catalog of known exploited vulnerabilities. These vulnerabilities carry significant risk to federal agencies as well as public and private sectors entities.
    - Implement rigorous **configuration management programs.** Ensure the programs can track and mitigate emerging threats. Regularly audit system configurations for misconfigurations and security weaknesses.
- **Monitor network logs for suspicious activity** and unauthorized or unusual login attempts.
    - Integrate SATCOM traffic into existing network security monitoring tools.
    - Review logs of systems behind SATCOM terminals for suspicious activity.
    - Ingest system and network generated logs into your enterprise security information and event management (SIEM) tool.
    - Implement endpoint detection and response (EDR) tools where possible on devices behind SATCOM terminals, and ingest into the SIEM.
    - Expand and enhance monitoring of network segments and assets that use SATCOM.
    - Expand monitoring to include ingress and egress traffic transiting SATCOM links and monitor for suspicious or anomalous network activity.
    - Baseline SATCOM network traffic to determine what is normal and investigate deviations, such as large spikes in traffic.
- Create, maintain, and exercise a **cyber incident response plan, resilience plan**, and continuity of operations plan so that critical functions and operations can be kept running if technology systems—including SATCOM networks—are disrupted or need to be taken offline.

Contact Information

All organizations should report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov or (888) 282-0870 and/or to the FBI via your local FBI field office or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Resources

- National Security Agency (NSA) Cybersecurity Advisory: Protecting VSAT Communications
- NSA Cybersecurity Technical Report: Network Infrastructure Security Guidance
- Office of the Director of National Intelligence (ODNI): Annual Threat Assessment of the U.S. Intelligence Community, February 2022
- CISA Tip: Choosing and Protecting Passwords
- CISA Capacity Enhancement Guide: Implementing Strong Authentication

Revisions

March 17, 2022: Initial Version
May 10, 2022: Added Atrribution