Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting

Russian Government-Sponsored Activity Targets Poorly Configured and Vulnerable Devices Across Critical Sectors

Executive summary

Russian Federal Security Service (FSB) Center 16 cyber actors continue to exploit poorly configured and vulnerable networking devices worldwide, opportunistically compromising multiple critical infrastructure sector networks. This joint Cybersecurity Advisory (CSA) builds on FBI's Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure Public Service Announcement of the decade-plus FSB Center 16 cyber activity by providing additional tactics, techniques, and procedures (TTPs) to enable defenders to more fully understand and counter the threat. [1]

This CSA is being released by the following authoring and co-sealing agencies:

- United States National Security Agency (NSA)
- United States Cybersecurity and Infrastructure Security Agency (CISA)
- United States Federal Bureau of Investigation (FBI)
- United States Department of Defense Cyber Crime Center (DC3)
- Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC)
- Communications Security Establishment Canada's (CSE's) Canadian Centre for Cyber Security (Cyber Centre)
- New Zealand National Cyber Security Centre (NCSC-NZ)
- United Kingdom National Cyber Security Centre (NCSC-UK)
- Czech Republic National Cyber and Information Security Agency (NÚKIB)[1]
- Danish Defence Intelligence Service (DDIS)[2]
- Estonian Foreign Intelligence Service (EFIS)[3]
- Estonian Information System Authority (RIA)[4]
- Finnish Defence Intelligence (FDI)[5]
- Finnish Security and Intelligence Service (SUPO)[6]
- French National Cybersecurity Agency (ANSSI)[7]
- Italian External Intelligence and Security Agency (AISE)[8]
- Italian Internal Intelligence and Security Agency (AISI)[9]
- The Military Counterintelligence Service of Poland (SKW)[10]
- Sweden National Cyber Security Centre (NCSC-SE)[11]

The authoring and co-sealing agencies strongly urge device owners and network defenders to take mitigation and remediation actions against Russian government-sponsored exploitation of vulnerable routers.

[1] Národní úřad pro kybernetickou a informační bezpečnost
[2] Forsvarets Efterretningstjeneste
[3] Välisluureamet
[4] Riigi Infosüsteem Amet
[5] Sotilastiedustelu
[6] Suojelupoliisi
[7] Agence nationale de la sécurité des systèmes d'information
[8] Agenzia Informazioni e Sicurezza Esterna
[9] Agenzia Informazioni e Sicurezza Interna
[10] Służba Kontrwywiadu Wojskowego
[11] Nationellt Cybersäkerhetscenter

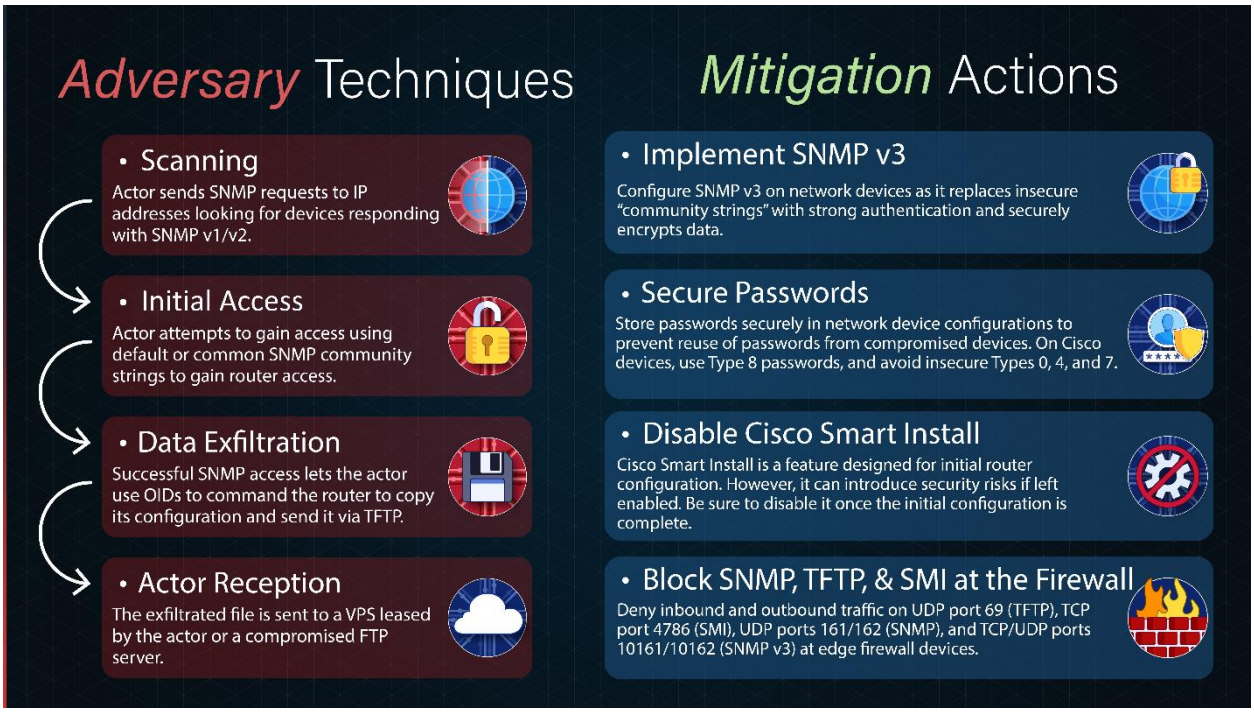

Figure 1: FSB Center 16 activity and recommended mitigation actions

Cybersecurity industry tracking

The cybersecurity industry provides overlapping cyber threat intelligence, indicators of compromise (IOCs), and mitigation recommendations related to this activity. Although not all encompassing, the following list contains the most notable threat group names commonly used within the cybersecurity community related to this activity:

- Berserk Bear
- Energetic Bear
- Crouching Yeti
- Dragonfly
- Ghost Blizzard
- Static Tundra

Note: Cybersecurity companies have different methods of tracking and attributing cyber actors, and this list may not provide a 1:1 correlation to the authoring agencies' understanding for all activity related to these groupings.

Targeting details

Critical infrastructure sectors most at risk from the Russian Federal Security Service (FSB) Center 16 cyber actors' targeting include:

- Communications,
- Defense Industrial Base,
- Energy,
- Financial Services,
- Government Services and Facilities, especially organizations at the state and local level, and
- Healthcare and Public Health.

Technical details

Note: This advisory uses the MITRE ATT&CK®[12] Matrix for Enterprise framework, version 19. See Appendix A for tables of the activity mapped to MITRE ATT&CK tactics and techniques. This advisory also uses MITRE DEFEND™ version 1.4.0.

The Russian FSB Center 16 cyber actors primarily use scanning to identify poorly configured networking devices, primarily routers, for exploitation. The actors scan for Internet IP ranges with active Simple Network Management Protocol (SNMP) agents that accept common or default community strings for authentication [T1595.001, T1595.002]. These scans, run via proxies, consist of SNMP Set-Requests from a spoofed IP address [T1027] containing Object Identifiers (OIDs) that instruct the SNMP agent on poorly configured networking devices to [T1569, T1602.001, T1090]:

- Copy its configuration to a file, often called "config.bkp" or "output.txt" [T1003, T1602.002].
- Transfer the file, typically using Trivial File Transfer Protocol (TFTP), to an actor-controlled leased virtual private server (VPS) or compromised FTP server [T1583.003, T1090, T1071, T1048].

While SNMP scanning is the primary method the actors use to discover and exploit poorly configured networking devices, they occasionally exploit common vulnerabilities and exposures (CVEs) in Cisco devices, Cisco's Smart Install (SMI) functionality, and

[12] MITRE and ATT&CK are registered trademarks of The MITRE Corporation. MITRE DEFEND is a trademark of the MITRE Corporation.

web portals to manage network devices. The actors previously exploited at least the following CVEs [T1584.008, T1588.005, T1190, T1068]:

- CVE-2018-0171
- CVE-2008-4128[13]

Many of these TTPs overlap with activity by other malicious cyber actors, such as Salt Typhoon. Even though this CSA focuses on Russian FSB Center 16 cyber activity, the mitigations below should detect and counter these and similar TTPs used by other actors.

Mitigation actions

The authoring agencies highly recommend network defenders implement the following mitigations to harden networks against this exploitation:

- Disable Cisco Smart Install on all devices [D3-ACH]. [2]
- Use SNMPv3 with "authPriv" configured to the most modern encryption standard that is supported by the device instead of SNMPv1 or SNMPv2 [D3-ACH]. [3]
    - Disable SNMPv1 and SNMPv2. These are legacy protocols and should no longer be needed on current devices. If they are necessary, change all community strings from defaults and only allow read-only community strings rather than read-write access.
    - SNMPv3 adds strong authentication and data encryption that are unavailable in SNMPv1 and v2. SNMPv3 replaces clear text shared passwords, known as community strings, with more securely encoded parameters, and authenticates and encrypts data [D3-MAN, D3-MENCR].
- Use strong, unique passwords for local accounts on network devices and configure credentials to be stored securely to prevent reuse of compromised passwords [D3-CH].
    - Cisco devices protect passwords in the configuration file using different hashing types. Use hashing type 8 for user credentials. Avoid using

[13] CVE-2008-4128 only affects end-of-life Cisco devices.

hashing type 0, 4, and 7 as they are insecure or store passwords in plaintext in the configuration file. [4]

  - Monitor for unusual credentials that do not conform to standard organizational naming conventions [D3-PM].
  - Monitor for and alert on logins using local accounts. Local accounts should only be used in emergency situations when accounts supported by centralized authentication servers are unavailable. Centralized authentication to network devices should support multi-factor authentication where feasible. [3]

- Monitor and restrict access to SNMP OIDs using a Management Information Base (MIB) allow list [D3-ACH]. [5] Reference the vendor-specific MIB for the network devices and monitor OIDs for indications of reconnaissance or misconfiguration in logs or intrusion detection systems (IDS). IDS rules should be written for inbound SNMP Set-Requests that contain OIDs targeting sensitive device data [D3-PM].
  - Example OIDs include:
    - 1.3.6.1.4.1.9.9.96.1.1 (Cisco Config Copy)
    - 1.3.6.1.4.1.9.9.96.1.1.1.1.5 (Config Copy Server Address, value for this OID is where the configuration file is being sent to)
- Restrict management protocols [D3-NTF].
  - Use Access Control Lists (ACLs) to only allow management protocols, such as SNMP, from management devices, preferably on an out-of-band network. [3]
  - On edge firewalls and devices deny all external communications on the following ports unless mission critical, with strict monitoring if blocking is not feasible:
    - User Datagram Protocol (UDP) port 69 (TFTP)
    - Transmission Control Protocol (TCP) port 4786 (SMI)
    - UDP ports 161 and 162 (SNMP)
    - TCP/UDP ports 10161 and 10162 (SNMPv3)

- Update network device software and firmware images, especially to patch known vulnerabilities, and upgrade end-of-life devices to supported ones.
    - Use an attack surface management service to identify and secure Internet-facing systems with weak configurations and known vulnerabilities [D3-NVA].
        - U.S.-based federal, state, local, tribal, and territorial governments and U.S. critical infrastructure organiztions should consider signing up for CISA's no-cost Cyber Hygiene services.
        - U.S. Defense Industrial Base organizations should consider signing up for NSA's DIB Cybersecurity Services.

Resources

United States:

- Russia Threat Overview and Advisories
- Network Infrastructure Security Guide

Canada:

- Routers cyber security best practices (ITSAP.80.019)
- Security considerations for edge devices (ITSM.80.101)
- Guidance on securely configuring network protocols (ITSP.40.062)
- Baseline security requirements for network security zones (ITSP.80.022)
- Top 10 IT security actions to protect Internet-connected networks and information (ITSM.10.089)

Works cited

[1] FBI. Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure. Alert Number: I-082025-PSA. 2025. https://www.ic3.gov/PSA/2025/PSA250820

[2] NSA. Cisco Smart Install Protocol Misuse. 2017. https://media.defense.gov/2019/Jul/16/2002157833/-1/-1/0/CSA-CISCO-SMART-INSTALL-PROTOCOL-MISUSE.PDF

[3] NSA. Network Infrastructure Security Guide. 2023. https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDE_20220615.PDF

[4] NSA. Cybersecurity Information Sheet Cisco Password Types: Best Practices. 2022. https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/0/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF

[5] NSA. Cybersecurity Information Sheet: Reducing the Risk of Simple Network Management Protocol (SNMP) Abuse. 2026. https://media.defense.gov/2026/Jul/09/2003959459/-1/-1/0/CSI_REDUCING_RISK_OF_SNMP_ABUSE.PDF

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.

Purpose

This document was developed in furtherance of the authoring agencies' cybersecurity missions, including their responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

United States organizations

- **National Security Agency (NSA)**
  Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
  Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
  Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov
- **Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigation (FBI)**
  U.S. organizations are encouraged to report suspicious or criminal activity related to information in this advisory to CISA via the agency's Incident Reporting System, its 24/7 Operations Center (report@cisa.gov or 888-282-0870), or your local FBI field office. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment user for the activity; the name of the submitting company or organization; and a designated point of contact.
- **United States Department of Defense Cyber Crime Center (DC3)**
  Defense Industrial Base Inquiries and Cybersecurity Services: DC3.DCISE@us.af.mil
  Defense Industrial Base mandatory cyber incident reporting as required by 10 U.S. Code Sections 391 and 393 and Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 is submitted at https://dibnet.dod.mil.
  Media Inquiries / Press Desk: DC3.Information@us.af.mil

Australian organizations

- **Australian Signals Directorate**

  Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.

Canadian organizations

- The Canadian Centre for Cyber Security (Cyber Centre), part of the Communications Security Establishment, encourages Canadian organizations to report cyber incidents and to strengthen the security of their networking devices.
  Report an incident or suspicious activity to the Cyber Centre by email at contact@cyber.gc.ca, online via the reporting tool Report a cyber incident - Canadian Centre for Cyber Security or by phone at 1-833-CYBER-88 (1-833-292-3788).

New Zealand organizations

- New Zealand National Cyber Security Centre (NCSC-NZ): info@ncsc.govt.nz

United Kingdom organizations

- Report significant cyber security incidents to ncsc.gov.uk/report-an-incident (monitored 24/7)

Estonia organizations

- Estonian Foreign Intelligence Service (EFIS): info@valisluureamet.ee

Finnish organizations

- Finnish Security and Intelligence Service: supo.fi/en/contact

French organizations

- French organizations are encouraged to report suspicious activity or incident related information found in this advisory by contacting ANSSI/CERT-FR at: cert-fr@ssi.gouv.fr or by phone at: 3218 or +33 9 70 83 32 18.

Italian Organizations

- Italian External Intelligence and Security Agency (AISE):
  Visit https://www.sicurezzanazionale.gov.it/
- Italian Internal Intelligence and Security Agency (AISI):
  Visit https://www.sicurezzanazionale.gov.it/

Appendix A: MITRE ATT&CK tactics and techniques

See **Table 1** through **Table 10** for all the threat actor tactics and techniques referenced in this advisory.

Table 1: Reconnaissance

Technique Title	ID	Use
Active Scanning: Scanning IP Blocks	T1595.001	Scan range of IP addresses
Active Scanning: Vulnerability Scanning	T1595.002	Scan victims for vulnerabilities that can be used during targeting

Table 2: Resource Development

Technique Title	ID	Use
Acquire Infrastructure: Virtual Private Servers	T1583.003	Leverage VPS as infrastructure
Compromise Infrastructure: Network Devices	T1584.008	Compromise intermediate routers
Obtain Capabilities: Exploits	T1588.005	Use publicly available code to exploit vulnerable devices

Table 3: Initial Access

Technique Title	ID	Use
Exploit Public-Facing Application	T1190	Exploit publicly known CVEs
Proxy	T1090	Use a connection proxy to direct network traffic

Table 4: Execution

Technique Title	ID	Use
System Services	T1569	Executing commands via SNMP

Table 5: Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Exploit publicly known CVEs for escalated privileges

Table 6: Stealth

Technique Title	ID	Use
Obfuscated Files or Information	T1027	Obfuscate source IP addresses in system logs, as actions may be recorded as originating from local IP addresses

Table 7: Credential Access

Technique Title	ID	Use
OS Credential Dumping	T1003	Collect router configuration with weak Cisco Type 7 passwords and Type 0

Table 8: Collection

Technique Title	ID	Use
Data from Configuration Repository: SNMP (MIB Dump)	T1602.001	Target MIB to collect network information via SNMP
Data from Configuration Repository: Network Device Configuration Dump	T1602.002	Acquire credentials by collecting network device configurations

Table 9: Command and Control

Technique Title	ID	Use
Proxy	T1090	Use VPS for C2
Application Layer Protocol	T1071	Open and expose a variety of different services, including TFTP and FTP

Table 10: Exfiltration

Technique Title	ID	Use
Exfiltration Over Alternative Protocol	T1048	Exfiltrating over a different protocol than that of the existing command and control channel.

Appendix B: MITRE D3FEND countermeasures

See **Table 11** for a mapping of several of the cybersecurity countermeasures mentioned in this advisory.

Table 11: MITRE D3FEND Countermeasures

Countermeasure Title	ID	Description
Application Configuration Hardening	D3-ACH	• Use SNMPv3 and disable SNMPv1 and SNMPv2. • Use SNMP allowlisting to restrict access to OIDs and MIBs. • Disable Cisco Smart Install.
Message Authentication	D3-MAN	• Use SNMPv3 with strong authentication.
Message Encryption	D3-MENCR	• Use SNMPv3 to encrypt payloads.
Credential Hardening	D3-CH	• Use strong, unique passwords and store them securely.
Platform Monitoring	D3-PM	• Monitor for unusual credentials. • Monitor SNMP Set-Requests for OIDs targeting sensitive device data.
Network Traffic Filtering	D3-NTF	• Use ACLs to only allow management protocols from management devices. • Block TFTP, SMI, and SNMP at edge firewalls.
Network Vulnerability Assessment	D3-NVA	• Use an attack surface management service.