OT-ISAC
OPERATIONAL TECHNOLOGY INFORMATION SHARING AND ANALYSIS CENTER

INFORMATION/SITUATIONAL AWARENESS ADVISORY

15 July 2026

Russian FSB Centre 16 Actors Continue Exploiting Vulnerable Routers Across Critical Infrastructure Sectors

AT A GLANCE

Threat Actor	FSB Centre 16 (aka Berserk Bear, Energetic Bear, Dragonfly, Static Tundra)
Activity	Scanning and exploitation of internet-exposed routers via weak/default SNMP, Cisco Smart Install and known Cisco CVEs
Sectors Named in Advisory	Defense Industrial Base, Communications, Energy, Financial Services, Government, Healthcare
OT/ICS Impact Confirmed?	No – advisory describes network-device compromise, not control-system manipulation
APAC Relevance	Moderate – co-sealed by Australia (ACSC) and New Zealand; elevated risk at distributed/remote sites
Action Required	Validate router/SNMP exposure and harden configurations this week

WHAT HAPPENED

On 13 July 2026, NSA, CISA, the FBI and the U.S. Department of Defense Cyber Crime Center, together with 14 international partner agencies including the UK NCSC and Australia's ACSC, published a joint advisory (AA26-194A) on ongoing Russian FSB Centre 16 exploitation of poorly configured and vulnerable routers worldwide.

Public reporting indicates the actors are scanning internet-exposed devices for SNMP services accepting common or default community strings, then using SNMP requests to command affected devices to copy their configuration and transfer it via TFTP to actor-controlled infrastructure. The advisory also cites exploitation of Cisco Smart Install, device web-management weaknesses and known Cisco vulnerabilities, and describes use of compromised routers and leased virtual private servers as proxy infrastructure.

The advisory identifies targeting across the Defense Industrial Base, communications, energy, financial services, government and healthcare sectors. Centre 16 is publicly tracked under several names, including Berserk Bear, Energetic Bear, Crouching Yeti, Dragonfly, Ghost Blizzard and Static Tundra.

WHY THIS MATTERS TO OT/ICS

OT-ISAC assesses this as a network-infrastructure reconnaissance and access risk rather than confirmed OT/process compromise. The advisory does not describe manipulation of PLCs, safety systems, control logic or physical processes.

The key member-facing concern is that routers and gateways frequently bridge corporate networks, OT DMZs, remote sites, telecommunications services and third-party support infrastructure. A compromised device can expose internal addressing, VPN relationships, access-control lists and credentials that could support reconnaissance or attempted movement toward jump hosts, remote-access servers, historians or engineering workstations – even without direct manipulation of the underlying industrial process. Malicious configuration changes could also degrade site connectivity or remote administration, reducing operational visibility.

For APAC operators: risk is likely elevated at geographically distributed or lightly staffed facilities that depend on remote administration, legacy network appliances or third-party connectivity. Australia and New Zealand co-sealed this advisory; it does not identify any confirmed OT-ISAC member impact.

Related development (context only): the same day, the UK and EU formally attributed a 29 December 2025 attack on Poland's energy grid – an attempted wiper-malware operation against distributed renewable energy assets – to Russia's FSB, with the UK specifically naming Centre 16. Attribution for that incident is not fully converged (Dragos assesses ELECTRUM/Sandworm overlap with moderate confidence; Polish and UK/EU government sources point to Centre 16/Static Tundra). OT-ISAC does not assess these as the same operation and is not asserting the router-hygiene activity above caused or enabled the Poland incident. It is noted as evidence this actor set has demonstrated intent and capability for OT-disruptive outcomes, supporting treatment of the router activity as a credible precursor risk.

WHAT MEMBERS SHOULD VALIDATE

- Whether any internet-facing routers, gateways or network-management interfaces are exposed, particularly at remote sites, OT DMZs or vendor-access points.
- Whether SNMPv1/v2c, Telnet, unauthenticated HTTP/HTTPS management, TFTP or Cisco Smart Install are reachable externally.
- Whether default, weak or shared SNMP community strings or administrative credentials remain in use.
- Recent administrator logins, configuration changes or configuration-copy activity on network devices, especially from unfamiliar hosts or locations.
- Unexpected TFTP/FTP transfers originating from routers or gateways.

WHAT ACTIONS SHOULD BE TAKEN NOW

- Disable SNMPv1 and SNMPv2c where operationally feasible; migrate to SNMPv3 with authentication and encryption.
- Replace default, weak or shared SNMP community strings and administrative passwords.
- Remove SNMP read-write access unless there is a documented operational requirement.
- Restrict management-plane access to authorised systems and administration networks.
- Disable Cisco Smart Install and other unused legacy management functionality.
- Apply vendor-approved firmware/software updates through established change-control and rollback processes.
- Review recent configuration-change and configuration-copy logs for anomalies; investigate unexpected TFTP/FTP transfers.

WHAT REMAINS UNCERTAIN

Confidence: High: that the router-targeting activity described in the joint advisory is ongoing.

Confidence: Medium: that distributed APAC critical-infrastructure operators face meaningful exposure, particularly at remote sites running legacy or externally managed network equipment.

Confidence: Low: regarding any direct OT-system access or operational impact from this specific reported activity – the advisory does not confirm control-system compromise.

The advisory notes actors may use proxies or spoofed source addresses; source IP information alone should not be treated as conclusive attribution. Attribution linking the Poland grid incident specifically to Centre 16 (versus ELECTRUM) is not yet fully converged across government and private-sector sources.

REFERENCES

[1] Improve Router Hygiene to Protect Against Russian State-Sponsored Targeting | CISA (AA26-194A)

[2] UK and Allies Urge Critical Sectors to Improve Defences Against Russian Intelligence Targeting | NCSC UK

In the spirit of community-driven effort, we'd like to encourage our Members and Partners to share information to enable our community to better defend itself and improve situational awareness. Most importantly – if your organization requires direct assistance from OT-ISAC, feel free to submit to OT-ISAC Member's Portal; our team will work with you to ensure all necessary support is available through the member submission and RFI process.