

UK and 12 Allies Issue Advisory on Russian FSB Targeting of Critical Infrastructure Routers



The UK National Cyber Security Centre and 18 agencies from 12 countries have published a joint advisory warning that Russian FSB Centre 16 is exploiting poorly configured routers to target critical infrastructure globally.

- Russian FSB Centre 16 is scanning the internet for routers with default or weak SNMP passwords and exploiting known Cisco vulnerabilities
- Communications, defence, energy, financial services, government and healthcare sectors face the highest risk from this global targeting campaign
- The joint advisory from 19 agencies across 13 countries recommends migrating to SNMPv3, implementing strong unique passwords and restricting management protocol access
- The warning coincides with UK sanctions against 24 entities and formal attribution of a December

2025 attack on Poland's energy grid to FSB Centre 16

- Organisations are urged to obtain Cyber Essentials certification and use the updated Cyber Assessment Framework to assess security maturity

The UK National Cyber Security Centre, alongside 18 partner agencies from Australia, Canada, Czech Republic, Denmark, Estonia, Finland, France, Italy, New Zealand, Poland, Sweden and the United States, has issued a joint cybersecurity advisory warning of active exploitation of network infrastructure by Russian state actors.

Threat Actor Methods

The advisory identifies **FSB Centre 16**, also tracked as Berserk Bear, Energetic Bear, Crouching Yeti, Dragonfly, Ghost Blizzard and Static Tundra, as conducting opportunistic scanning of internet-facing routers to identify devices configured with default or weak **Simple Network Management Protocol** passwords and community strings. The threat actor has also exploited known vulnerabilities in Cisco devices, the Smart Install feature and web-portal flaws to gain control of network equipment.

The targeting is global in scope and focuses on organisations operating in communications, defence, energy, financial services, government and healthcare sectors. The UK and EU member states have formally attributed a December 2025 attack on Poland's energy grid to this actor, noting the attack could have disrupted electricity supply to 500,000 civilians.

Recommended Technical Controls

The advisory recommends organisations migrate to SNMPv3 and disable legacy SNMP versions, implement strong and unique passwords for all network devices, and restrict access to management protocols through appropriate access controls. The NCSC also encourages organisations to obtain Cyber Essentials certification and utilise the updated Cyber Assessment Framework to assess security maturity and address vulnerabilities.

The coordinated disclosure accompanies UK government sanctions against 24 individuals and entities involved in destructive cyber and hybrid operations linked to Russian Intelligence Services.

What to do now

1. Conduct an immediate inventory of all internet-facing routers and network devices to identify equipment using default or weak SNMP configurations
2. Migrate network management protocols to SNMPv3 and disable SNMPv1 and SNMPv2c on all infrastructure devices
3. Implement strong, unique passwords for all network device administrative accounts and change default community strings
4. Review and restrict access to management protocols (SNMP, SSH, Telnet) through network segmentation and access control lists

5. Audit Cisco devices for known vulnerabilities, disable Smart Install feature where not required, and apply vendor security patches
6. Assess current security posture against the NCSC Cyber Assessment Framework and consider Cyber Essentials certification for baseline controls