UK and Allies urge critical sectors to improve defences against Russian intelligence targeting

**New advisory highlights Russian state cyber actors' global exploitation of poorly configured routers **

- The UK and international allies strongly urge action to better defend against the threat from Russian state intelligence actors
- Advice follows the opportunistic exploitation of inadequately configured routers and network devices by Centre 16 of Russia's Federal Security Service (FSB)
- Warning comes as the UK sanctions Russian state and criminal networks for cyber and hybrid operations and calls out the FSB for a reckless attack on Poland's energy grid.

Organisations in critical infrastructure sectors are being supported to better understand and defend against malicious activity, as the UK and international partners today call out techniques used by Russian Intelligence Services

Alongside 18 agencies from 12 countries, the National Cyber Security Centre (NCSC) – a part of GCHQ – has published a new advisory highlighting the methods of Federal Security Service (FSB) Centre 16 cyber actors, who are exploiting vulnerable routers and opportunistically targeting networks belonging to critical national infrastructure (CNI) globally.

Sectors most at risk from this global targeting, including communications, defence, energy, financial services, government and healthcare, are subsequently being urged to take action. This includes recommendations to use SNMPv3 and disable legacy SNMP versions, implement strong and unique passwords for network devices, and restrict access to management protocols through appropriate access controls.

Centre 16, also known as Berserk Bear, Energetic Bear, Crouching Yeti, Dragonfly, Ghost Blizzard and Static Tundra, has been seen hunting for vulnerable routers by scanning the internet for devices that still use default or weak Simple Network Management Protocol (SNMP) passwords and community strings.

Whilst the actor primarily uses SNMP scans to locate and compromise vulnerable routers, they have also exploited well-known vulnerabilities relating to Cisco devices, Cisco's Smart Install (SMI) feature and web-portal flaws to gain control of network devices.

Jonathon Ellison, NCSC Director of National Resilience said:

> *The NCSC, alongside our international partners, have repeatedly exposed the advanced tools and coordinated campaigns of Russian cyber actors who persistently seek to exploit any vulnerability they encounter.*
>
> *"Today's joint advisory provides decisive, actionable directions from the global security community that network defenders should implement to protect against Russian Intelligence operations and secure the UK's critical infrastructure.*
>
> *"I'd strongly encourage all organisations, especially those entrusted with UK critical networks, to adopt these recommended measures immediately, thereby reducing the risk of compromise.*

Organisations are also encouraged to obtain Cyber Essentials certification, the government-backed scheme for all organisations to show they meet the recognised UK minimum standard for cyber security, and make use of the updated Cyber Assessment Framework, enabling them to assess their security maturity, address vulnerabilities and build their resilience against increasing threats.

The advisory has been published on the same day as the UK government has sanctioned 24 individuals and entities behind destructive cyber and hybrid operations including cyber criminals involved in proxy networks linked to the Russian Intelligence Services.

The UK together with EU member states has also today formally attributed the December 2025 attack on Poland's energy grid to Russia's FSB Centre 16 – an attack that if it had been successful could have caused 500,000 civilians to lose electricity.

The NCSC has co-sealed this new advisory alongside agencies from Australia, Canada, Czech Republic, Denmark, Estonia, Finland, France, Italy, New Zealand, Poland, Sweden and the United States.

It can be read on the NSA website:
https://media.defense.gov/2026/Jul/09/2003959498/-1/-1/1/CSA_IMPROVE_ROUTER_HYGIENE.PDF

PUBLISHED

13 July 2026

NEWS TYPE

General news