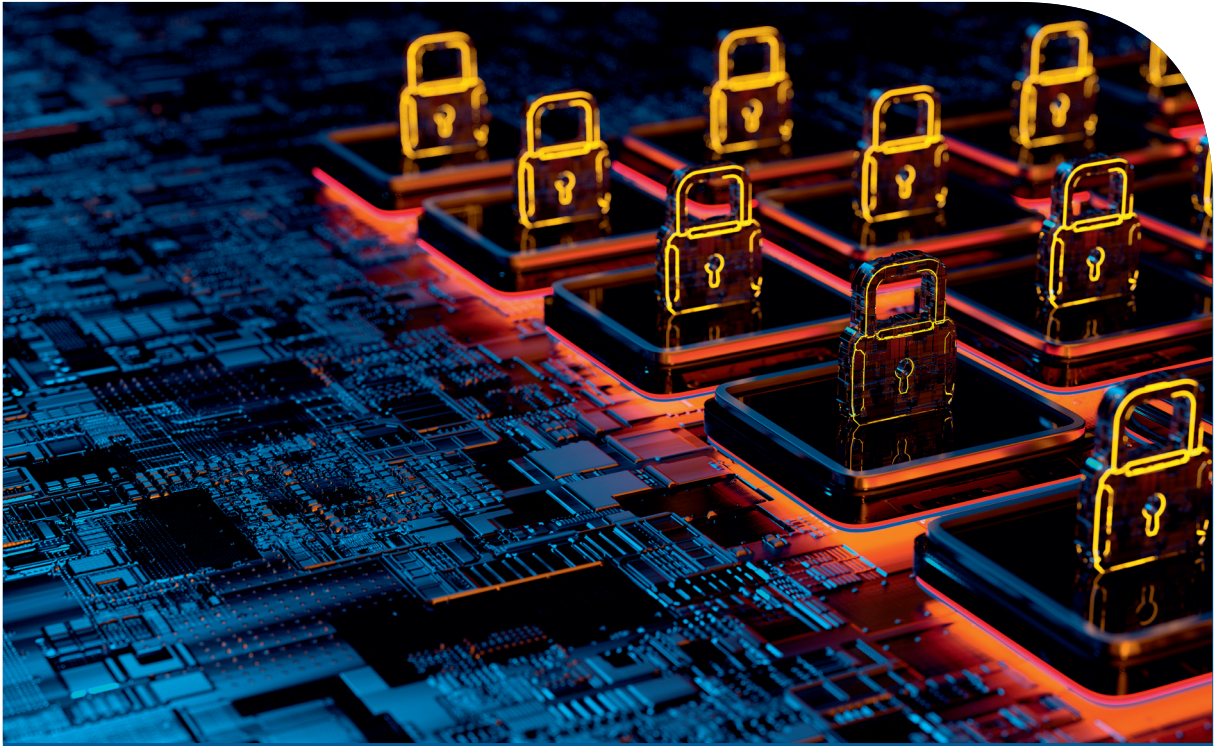




Cyber Advisory

*Edge devices systematically targeted
by Chinese cyber threat actors*

General Intelligence and Security Service (AIVD)

Military Intelligence and Security Service (MIVD)

National Cyber Security Centre (NCSC)

october 2026

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

Key points

- The Netherlands Defence Intelligence and Security Service (MIVD) has previously highlighted an expected increase in Chinese cyber campaigns targeting vulnerabilities in *edge devices*, as noted in its 2025 public annual report.
- Chinese actors are investing in deep-level technical expertise of *edge devices*.
- Beyond *reverse engineering* and targeted research into Western products, Chinese threat actors also utilise cyber espionage to acquire critical insights into technical specifications. A prime example is their possession of the source code of specific Western products.
- The convergence of deep-level technical expertise of Western products (including source code access), intensive support from a diverse ecosystem of Chinese commercial entities and knowledge institutions, and advancements in artificial intelligence (AI) in the cyber domain is expected to drive an escalation in the exploitation of *edge devices* by Chinese actors.
- Beyond the discovery and exploitation of a large number of zero-day vulnerabilities annually, the convergence of these drivers further enables Chinese threat actors to rapidly operationalise known vulnerabilities as part of their cyber tradecraft.
- Consequently, organisations must prepare for threats from known or recently disclosed vulnerabilities as well as from zero-day vulnerabilities.
- Organisations must also balance the necessity of rapid mitigation against the risk of application or system instability. The risk of exploitation and subsequent impact can be mitigated through a multi-layered approach, specifically through *defence-in-depth*, vendor diversification, centralised logging, *robust security monitoring and response*, and *forensic readiness*.

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

Context

Exploitation of vulnerable *edge devices* by Chinese actors

The Netherlands Defence Intelligence and Security Service (MIVD) has previously highlighted an expected increase in Chinese cyber campaigns targeting vulnerabilities in *edge devices*, as noted in its 2025 public annual report.¹ *Edge devices* – such as firewalls, proxies, portals, and VPN gateways – sit at the network perimeter. This inherent internet exposure means these devices constitute a critical attack surface for external actors. Although many cyber threat actors are known to exploit edge device vulnerabilities, it is recognised as an established MO of Chinese cyber threat actors. Chinese threat actors have exploited vulnerable *edge devices* to breach numerous networks in recent years, with organisations in the Netherlands among the documented cases.

This advisory examines the drivers behind the escalating exploitation of vulnerable *edge devices* by Chinese actors – and the subsequent warnings they trigger – while outlining essential mitigation strategies for organisations.

Factors driving the escalating exploitation of *edge devices*

Systematic reverse-engineering of Western-manufactured *edge devices* by Chinese threat actors enables them to acquire the deep-level expertise needed to identify and exploit device vulnerabilities. Chinese actors also utilise cyber espionage, notably covertly obtaining the source code of certain Western-manufactured *edge devices* to identify their vulnerabilities.

In 2021, China introduced legislation compelling actors to report vulnerabilities. China has also developed specific training programmes and established knowledge institutions specifically for the purpose of exploit development in relation to *edge devices* routinely used in Western digital infrastructure. Moreover, beyond targeted research into Western product vulnerabilities, Chinese commercial entities also produce ready-to-use, ‘weaponised’ exploits. This ecosystem enhances China's body of knowledge about Western digital infrastructure vulnerabilities, while simultaneously strengthening the capability of Chinese actors to execute offensive cyber operations against Western targets.

¹ MIVD in partnership with NCSC-NL previously warned of large-scale exploitation of *edge devices* throughout the COATHANGER campaign.

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

In their 2025 public annual reports, the Netherlands Defence Intelligence and Security Service (MIVD) and the Netherlands General Intelligence and Security Service (AIVD) highlighted opportunities that artificial intelligence (AI) presents in the cyber threat domain. The development and availability of AI is expected to contribute to an escalation in exploitation of vulnerable *edge devices*, including by Chinese actors.

Beyond the discovery and exploitation of a large number of zero-day vulnerabilities annually, the convergence of these drivers further enables Chinese cyber actors to rapidly operationalise known vulnerabilities.

The implications of source code access for actors

Access to a product's underlying source code provides threat actors with the understanding needed to perform thorough reverse engineering and identify exploitable flaws within the product's source code. From here, the actor can build attack tools to exploit zero-day vulnerabilities. Support from the Chinese ecosystem, bolstered by the integration of AI into source code analysis, facilitates a more rapid and efficient exploitation cycle.

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

Recommendations

This advisory does not offer total protection against the exploitation of zero-day or documented vulnerabilities. Rather, it intends to provide an actionable framework to mitigate the risk of compromise and reduce the impact of a successful breach. The foundational step is to identify and categorise your organisation's critical assets ('crown jewels') to ensure they are adequately protected against targeted exploitation.²

Managing vulnerabilities

Following disclosure of a vulnerability in a particular type of edge device, the risk of exploitation increases exponentially. Intelligence from the AIVD and MIVD indicates that Chinese actors leverage both zero-day exploits and known vulnerabilities. Consequently, regular implementation of vendor security updates is essential. Nevertheless, given the potential impact on production environments, updates should be rigorously tested before deployment. Organisations must balance the necessity of rapid mitigation against the risk of application or system instability.

The actionable framework offered here is primarily intended to mitigate the risk of zero-day vulnerabilities or to mitigate the risk of documented vulnerabilities in situations where it is not possible to deploy security updates.

² Further reading at: <https://www.ncsc.nl/en/risk-management>

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

Defence in depth

Defence in depth is effective in mitigating the impact of a network breach and facilitating rapid detection. This model represents a layered approach to network and information security. If one security layer fails, the other layers will block or delay the attack.

Examples (non-exhaustive) of *defence in depth* include:

- Custom-configured firewalls
- *Intrusion detection systems*
- Organisation-wide multi-factor authentication
- Network segmentation
- Multi-layered data encryption across the network

Implementing vendor diversification policies across the layered network defences is a further key recommendation. The resulting multi-vendor architecture can help bolster defences and reduce the impact of targeted research into specific product lines, ensuring that a successful exploit against one vendor does not breach multiple security layers.

Detection and incident management

Centralised logging

Experience shows that victims of security incidents are often unable to produce sufficient log files. Logs are either not routinely stored or the retention period is extremely short. Experience also reveals that incident logs are routinely stored locally on the exploitable devices. Once a device has been compromised, local log file manipulation or deletion becomes trivial for an attacker.

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

Establishing a centralised logging system in an isolated network segment, for example in a segment reserved for the Security Operations Centre (SOC), is a key recommendation. Enforcing a centralised logging policy for critical networked devices ensures that post-incident impact assessment and forensic analysis is not impeded by missing or lost logs. Furthermore, establishing longer log file retention periods is critical. Implementing a policy stipulating a retention period of at least six months, but preferably a year or longer, is therefore a key recommendation.

Security monitoring and response

Organisations should maintain a mature and robust network security monitoring ecosystem, supported by a highly trained and specialised SOC. Effective security monitoring, rapid detection of anomalous network activity and appropriate response are critical in minimising the operational impact of a breach. To bolster the effectiveness of these capabilities, organisations should periodically test internal attack paths through red-team exercises to validate the SOC's detection and response proficiency.

Forensic readiness

Following a cyber incident, organisations are frequently ill-equipped to conduct a thorough digital forensic investigation. To mitigate this risk, organisations should implement forensic incident investigation and readiness policies, sustained through robust staff training and periodic incident response exercises.

Such preparedness enables a more rapid and effective investigation, not only lowering the total cost of incident investigation but also shortening the digital forensic investigation lifecycle.

Analysis of the overall impact of incidents on the organisation and its infrastructure ('*damage assessment*') helps organisations adopt appropriate measures to effectively mitigate incidents and achieve forensic readiness.

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

Further reading

Consult the following resources for more in-depth information:

- AIVD, Verdedigbaar Netwerk – Hoe doe je dat?, 19 augustus 2024, www.aivd.nl/documenten/2024/08/19/aivd-publicatie-verdedigbaar-netwerk-hoe-doe-je-dat.
- AIVD/MIVD, Logging Essentials, <https://github.com/JSCU-NL/logging-essentials>.
- NCSC, Infosheet Basismaatregelen, d.d. 1 oktober 2023, www.ncsc.nl/documenten/publicaties/2023/december/01/infosheet_basismaatregelen.
- NCSC, Disaster Recovery Plan, d.d. 5 februari 2026, www.ncsc.nl/incidenten-en-herstellen/disaster-recovery-plan.
- NCSC, Beheerlijst voor Edge Devices, d.d. 15 januari 2026, www.ncsc.nl/edge-devices/beheerlijst-voor-edge-devices.
- NCSC, SOC van de Toekomst, d.d. 9 december 2025, www.ncsc.nl/incidenten-en-herstellen/soc-van-de-toekomst.
- NCSC, Bent u al klaar voor Forensic Readiness?, d.d. 12 mei 2021, www.ncsc.nl/actueel/weblog/weblog/2021/bent-u-al-klaar-voor-forensic-readiness.
- NCSC, Bereid u voor op Zero Trust, d.d. 18 augustus 2021, https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2021/augustus/18/factsheet-bereid-u-voor-op-zero-trust/Factsheet_bereid+u+voor+op+Zero+Trust+v1.0_aug21_NL.pdf.
- NCSC, Factsheet SOC inrichten, d.d. 3 mei 2023, www.ncsc.nl/documenten/factsheets/2019/juni/01/soc-inrichten.
- NCSC, Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices, d.d. 10 juni 2024, www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-stataelijke-cyberspionagecampagne-via-kwetsbare-edge-devices.

Cyber Advisory

Edge devices systematically targeted by Chinese cyber threat actors

About this Cyber Advisory

The AIVD and MIVD regularly publish advisories derived from the intelligence investigations of both agencies. These publications can be viewed on the website of the Ministry of Defence (for the MIVD) and the AIVD's own website. The objective of this advisory is to enhance resilience by providing stakeholders with an actionable framework of security measures, developed in close coordination with NCSC-NL. With a strategic focus on European security, these measures are derived from assessed threat intelligence, technical knowledge and subject-matter expertise.

Distributions

This document is labelled **TLP:CLEAR**

Subject to applicable copyright laws and information disclosure regulations and procedures, TLP:CLEAR information may be distributed without restriction.

General Intelligence and Security Service (AIVD)
english.aivd.nl

Military Intelligence and Security Service (MIVD)
ministryofdefence.nl

National Cyber Security Centre (NCSC)
ncsc.nl/en

october 2026