National Cyber
and Information
Security Agency

NÚKIB

National Cyber and Information Security Agency
Mučednická 1125/31
616 00 Brno – Žabovřesky
Business ID No.: 05800226
Data box ID: zzfnkp3

File ref. No.:
350-544/2025-E
Reference No.:
4417/2025-NÚKIB-E/350

Brno, 9 July 2025

WARNING

The National Cyber and Information Security Agency, registered office: Mučednická 1125/31, 616 00 Brno (hereinafter the “Agency”), pursuant to Section 12(1) of Act No. 181/2014 Coll., on cyber security and on amendments to related acts, as amended (hereinafter the “Cyber Security Act”), issues the following

warning

of cyber security threat consisting of the use of products, applications, solutions, websites and web services, including application programming interfaces, provided by Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. or any of its predecessor, successor, parent, subsidiary or affiliated companies (hereinafter referred to collectively as the “Affected Products”), on devices accessing information and communication systems of critical information infrastructure, information systems of essential services and important information systems. This warning does not apply to security testing, research and analysis of the Affected Products or to Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd.´s open-source large language models, the entire source code of which is publicly available and analysable, if the model is deployed locally without the ability to communicate with servers used by Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. or any of its predecessor, successor, parent, subsidiary or affiliated companies.

The Agency has evaluated this threat as **High - The threat is likely to very likely**.

Authorities and persons who are obliged to implement security measures pursuant to the Cyber Security Act are obliged to evaluate this threat in the context of risk management pursuant to Section 5(1)(d) of Decree No. 82/2018 Coll., on security measures, cyber security incidents, reactive measures, cyber security filing requirements and data disposal (hereinafter the “Cyber Security Decree”), at the level of High - The threat is likely to very likely. If an obliged person uses another method for risk evaluation in accordance with Section 5 of Annex 2 to the Cyber Security Decree, the threat must be assessed at a comparable level as would be the case in the procedure pursuant to Article 5(1)(d) of the Cyber Security Decree.

REASONING

1. Section 11(1) of the Cyber Security Act defines measures (actions taken to protect against or address a cyber security threat or incident), which, pursuant to Section 11(2)(a) of the Cyber Security Act, include, inter alia, warnings. According to Section 12(1) of the Cyber Security Act, the Agency issues a warning if it learns of a cyber security threat.

2. Based on facts established during the exercise of its powers, supplemented by unclassified and classified information obtained from domestic and foreign partners, the Agency concluded that the use of the Affected Products, as described above in the operative part of this warning, constitutes a cyber security threat and therefore it issues this warning pursuant to Section 12(1) of the Cyber Security Act.

3. A combination of the following observations and findings led to the issuance of this warning.

4. When assessing whether the above-mentioned Affected Products of Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd. (hereinafter "DeepSeek") – although this applies generally to the assessment of cyber security of any technology – pose a threat to the Czech Republic from the cyber security perspective, it is necessary to examine not only the technical aspects of such Affected Products, but also the broader context of their operation, including, for example, the legal environment from which the products in question originate. The trustworthiness level of countries' legal environments has a direct impact on the trustworthiness of the companies that reside in them and are subject to such legal environments. In some cases, this may provide fundamental reasons to question the trustworthiness of the products themselves.

5. The Affected Products of DeepSeek were developed and are further operated by DeepSeek, a company based in the People's Republic of China (hereinafter the "PRC"), which is therefore unreservedly subject to the legal environment of that country. For this reason, DeepSeek is subject to certain legal regulations of the PRC, which, in combination with the other findings (listed below), are problematic from the perspective of the Czech Republic's security.

6. They include the National Security Law (国家安全法) of 2015, which imposes a general duty on all Chinese citizens and organisations to provide assistance to state authorities in matters of state security. In addition, the National Intelligence Law (中华人民共和国国家情报法) of 2017 stipulates in Article 7 that every citizen and organisation must support national intelligence activities, provide cooperation and collaboration, and maintain confidentiality regarding classified matters that come to their attention in connection with national intelligence activities. Furthermore, the Counter-Espionage Law (中华人民共和国反间谍法) of 2014 imposes the duty to provide cooperation and information on foreign clients of Chinese companies in case they are suspected of espionage activities by state authorities, and according to Article 6, this law also applies to institutions, organisations and individuals who organise or finance espionage activities against the PRC outside its territory, where a wide range of activities can be defined as espionage by the Chinese authorities, all without the possibility of independent judicial review. Another of these regulations is the Company Law (

中华人民共和国公司法 2013修订) of 2013, which allows the Communist Party of China (CPC) to effectively influence the operation of private companies. According to Article 19, a CPC organisation must be established in a company for the purpose of carrying out CPC activities in accordance with its articles of association, and a company must ensure the necessary conditions for these activities. The rules for reporting vulnerabilities in network products (公安部关于印发网络产品安全漏洞管理规定的通知) from 2021 are also problematic, according to which technology manufacturers are required to report security vulnerabilities to the Chinese Ministry of Industry and IT (hereinafter the “MIIT”) within two days of their discovery. The MIIT then reports such findings to the PRC Ministry of State Security and other relevant institutions, and technology manufacturers are prohibited from disclosing or reporting these vulnerabilities to foreign organisations and individuals.

7. The above creates reasonable concerns that the interests of the PRC may be placed above the interests of users of technologies from companies subject to the PRC legal environment, including DeepSeek, as a producer of the Affected Products, through active coercion by the PRC government.

8. In addition, the Chinese state can interfere with the operation and structures of many formally private companies through ownership interests (so-called Golden Shares), and state supervision of such companies is further deepened by the activities of CPC organisations, which are compulsorily established in these companies based on the aforementioned Company Law (中华人民共和国公司法 2013修订) of 2013. The findings of the Agency’s partners confirm that the CPC influences decision-making processes, for example regarding the appointment of the company employees.

9. DeepSeek´s deeper ties to the PRC government are indicated by the participation of Liang Wenfeng, founder of DeepSeek and its parent company High-Flyer Technology, at a symposium hosted by PRC Prime Minister Li Qiang. This conclusion is further supported by other facts (set out below) relating to both DeepSeek and High-Flyer Technology.

10. The parent company High-Flyer Technology, as well as DeepSeek´s two branches in Hangzhou and Beijing, are located in technologically very important locations. The Hangzhou technology corridor is a project carried out under the auspices of the PRC government that centrally manages and subsidises the development of this innovation centre over the long term. This is directly reflected in support for local private companies engaged in AI research and development.

11. Another indicator of DeepSeek´s deeper ties with the PRC government is that DeepSeek´s parent company, High-Flyer Technology, was designated as a national high-tech enterprise in 2020 and 2023. High-Flyer Technology is a hedge fund and is currently China’s largest quantitatively managed fund. In the PRC, a hedge fund, which High-Flyer Technology has been since 2015, cannot be managed without the approval and control of the CPC.

12. In the context of assessing the security threat posed by the Affected Products of DeepSeek to the Czech Republic, it is impossible to ignore the fact that DeepSeek´s founder, Liang Wenfeng,

was probably also involved in research on dual-use technologies through his university professor, Xiang Qiyu, who is a prominent expert on artificial intelligence, connected vehicles and computer vision. In this context, it should be noted that Xiang Qiyu has published studies and holds patents on, among other things, the operation of autonomous vehicles in battlespaces with unpredictable terrain.

13. This warning is also issued in light of the fact that the Czech Republic has long been a target of Chinese cyber state actors. In recent years, the Agency has observed campaigns by actors associated with the Ministry of State Security and the PRC military, targeting both government and private entities, as well as individuals directly in the Czech Republic. The implementation of these activities by the PRC against the Czech Republic is evidenced, among other things, by the malicious cyber campaign conducted by the APT31 group, which is associated with the Chinese intelligence service of the Ministry of State Security. This group has been attacking one of the unclassified networks of the Czech Ministry of Foreign Affairs since 2022. The conclusions of the analysis carried out by the Agency, Military Intelligence, the Office for Foreign Relations and Information and the Security Information Service clearly show that the PRC and the APT31 group (also known as Zirconium or Judgment Panda), which is associated with a number of attacks against political and other targets, among others, on the territory of other EU Member States and NATO Allies, are behind this long-lasting malicious campaign.

14. Given the previous espionage activities, actions against the national interests of EU Member States and NATO Allies, the specifics of PRC legislation described above and the influence of the PRC government in Chinese companies, it is highly likely that the PRC will use the capabilities of DeepSeek´s products for intelligence activities. The Security Information Service repeatedly draws attention to these influential activities in the Czech Republic in its annual reports.

15. As of 4 April 2025, ten countries and territories have already issued measures against DeepSeek´s products (Italy, the Netherlands, Denmark, Norway, Australia, Canada, Taiwan, South Korea, India and some US states, such as Texas, Virginia and New York) due to national security concerns and doubts about data protection compliance. Given the composition of this group of countries, it is clear that the concerns about DeepSeek´s products do not stem solely from a shared cultural environment or the geographical location of these countries, but they are rather a response following an objective identification and evaluation of the risk posed by these products. Moreover, it is almost certain that other countries will introduce measures against DeepSeek´s products in the coming months. As part of these measures, countries most often resort to bans or restrictions on the equipment of state or government employees. However, in the case of Italy and South Korea, DeepSeek´s products were removed from, for example, app stores that ordinary citizens in those countries come into contact with. Academic institutions and private companies around the world are also resorting to bans, also because of security and data protection risks.

16. The level of security risk stated by this warning also results from a technical analysis of the DeepSeek mobile app, where the accumulated knowledge about the app's functioning also clearly supports the Agency's conclusion on the necessity of issuing this warning.

17. In fact, DeepSeek´s mobile app almost certainly collects all the content that the user provides to both the chatbot and the associated services. It also collects data about the user or a particular device, all of which is stored on servers in the PRC, where all of these data and information can be accessed by Chinese government authorities. In addition, DeepSeek does not specify the period of time for which these data are stored on the servers, or whether they are ever deleted. According to available information, these data are also being transferred to the servers of Huawei and China Mobile, among others – companies sanctioned by the Czech Republic's partners. The Agency has also issued a warning against Huawei. There is evidence that the data in question was also shared with ByteDance, which developed and continues to operate the TikTok app, in relation to which the Agency has also issued a warning in the past. This information is also confirmed by the Agency's internal analysis. In addition, according to a partner of the Agency, DeepSeek´s mobile app also sends data to servers managed by Zhejiang Taobao Network Co. Ltd in the territory of the Russian Federation.

18. Beyond the justification for this warning, the Agency, for the purpose of enabling a comprehensive assessment of the threat posed by the affected products of DeepSeek, considers it appropriate to mention that DeepSeek's products are also demonstrably subject to censorship by the PRC government, thereby aiding in the dissemination of pro-Chinese propaganda. Evidence of such activity by the chatbot is the documented and proven distortion of information in favour of Chinese political narratives, resulting in the provision of deliberately misleading information that may not be obviously incorrect at first glance. This may lead to the purposeful and intentional influencing of users' perceptions and opinions in favour of the PRC. A clear example of the censorial tendencies of DeepSeek's products is, for instance, the refusal to provide information about the events that occurred in Beijing's Tiananmen Square or the dissemination of information promoting the Communist Party of China's narrative regarding Taiwan's independence. All this information demonstrates that the affected products and DeepSeek itself are subject to the influence and control of the PRC government.

19. In addition to the risks associated with sending data, the mobile app itself also poses a security risk, especially when used by employees who handle sensitive information or hold important positions. DeepSeek´s mobile app has many security risks in the form of insufficient security of data transmission and handling, as well as the collection of such types of data that, in large quantities, may lead to the de-anonymisation of specific individual users. Technical analyses of both the Android and iOS versions of DeepSeek´s mobile app simultaneously show insufficient security against cyber attacks.

20. DeepSeek´s iOS mobile app collects a wide range of data about users and the device itself (called fingerprinting), some of which it sends unencrypted by disabling App Transport Security, a feature in the device that is designed to prevent the transmission of unencrypted data. According to an analysis by the Agency's partners, similar protections are also disabled in the Android version of the mobile app. Although separately this data does not pose a fundamental risk, once the data points are aggregated, it is possible to identify specific individuals, which can be used to build profiles of persons of interest. Data points collected by DeepSeek´s mobile app include region, time zone, language, access method (e.g. via Wi-Fi), operating system, device model, processor model or device name. For iOS, the device name is

in some cases automatically set as the customer's name, which is very risky given the above-mentioned. In the December 2024 Privacy Policy, DeepSeek also declares the collection of keystroke and rhythm data (which is no longer in the updated February 2025 policy). DeepSeek´s iOS mobile app also contravenes other principles of good practice by, among other things, using outdated encryption methods or risky handling of encryption keys, which can be exploited, for example, for man-in-the-middle attacks aimed at intercepting communications. All of these conclusions are confirmed by the analysis of the Agency's partners.

21. Another risk factor for the iOS version of DeepSeek´s mobile app is the use of the outdated 3DES encryption algorithm, the repeated use of initialisation vectors and hardcoding. The use of outdated encryption greatly facilitates and increases the speed of data decryption. Encryption keys embedded directly into the code allow real-time decryption. Initialisation vectors should be unique and unpredictable, and it is their repeated use that reduces the level of security.

22. Last but not least, the Agency also perceives the possibility of the recovery of sensitive data from a device's cache (cached database) as a risk that attackers can exploit, especially if they gain physical access to a device. In this way, attackers can gain access to, for example, login details and passwords.

23. In the case of the Android version of DeepSeek´s mobile app, the mobile app has weak root detection, which can make it easy for attackers to gain covert access to an entire device. Rooting allows all user applications to run privileged commands that cannot run when the device is configured initially. Weak rooting detection then leads to the inability to detect if the device has been switched to privileged mode, which allows access to essentially all device functions. Attackers with such access can therefore bypass security controls. Rooted devices are therefore highly vulnerable to malware. The above follows from the Agency's internal analysis.

24. Furthermore, DeepSeek´s mobile app for Android lacks appropriate network security measures and is therefore highly vulnerable to man-in-the-middle attacks. If a user connects over public Wi-Fi or an untrusted network, attackers can intercept and manipulate data, or steal login credentials, personal messages and payment information.

25. The Android version of DeepSeek´s mobile app is also at risk due to the lack of SSL certificate authentication, which makes the app vulnerable to fake websites or unauthorised access. Attackers can therefore impersonate trusted servers and, thanks to the aforementioned non-authentication of SSL certificates, intercept sensitive information such as login credentials and personal data.

26. DeepSeek´s Android mobile app also has the StrandHogg vulnerability, which allows malicious apps to take over the tasks of legitimate apps, display fake login screens and steal user login credentials. Further, the mobile app is also vulnerable to the Janus vulnerability, which allows attackers to modify the app's APK file without breaking its digital signature, allowing malware insertion. Last but not least, DeepSeek´s Android version of its mobile app is also susceptible to a method known as tapjacking, which aims to trick users into granting dangerous permissions by overlaying invisible UI elements on legitimate buttons.

27. As far as the DeepSeek web client is concerned, it allows requests to models on servers in the PRC, where, in light of the above-mentioned information not only about the PRC legal order but also about the PRC's undesirable activities towards the Czech Republic, the main risk lies in sending the entered data to the PRC and in accessing browser data. It should be pointed out that DeepSeek´s publicly accessible database for the web client, which was discovered by cyber security analysts just days after the public launch of the R1 large language model (also available as a mobile app), was insecure. The database thus allowed full control over database operations, including the ability to access internal data, and contained more than a million lines of logs containing chat history, secret keys, details of the backend (which is the application used for administration) and other highly sensitive information.

28. The scope of this warning also includes DeepSeek´s application programming interface (API), which is a tool for integrating DeepSeek´s products into third-party product applications. The interface allows applications to send model data and receive back processed responses, usually over http. The interface in question is very risky in light of the facts described above in this warning, as it sends data to servers in the PRC, and it may not be apparent that a third-party application is using DeepSeek´s services. Currently, DeepSeek´s products are integrated into the systems and activities of at least 20 Chinese state-owned enterprises in sectors such as energy, communications, finance and construction, and are also used by Chinese companies such as Lenovo and Tencent. The R1 large language model is also incorporated as part of these companies' products. Almost twenty other Chinese companies operating in the automotive industry, some of which are joint ventures with Western brands, have already signed strategic partnerships with DeepSeek. Further, it is very likely that Western companies without any business connection to the PRC will implement DeepSeek´s products in their systems, especially if the PRC adopts its usual strategy of dumping prices, i.e. selling below cost. It is very likely that some types of data will be shared with DeepSeek through this integration. Therefore, the skewing of results in favour of Chinese narratives will be able to trickle down to third-party applications that do not originate in the PRC, and DeepSeek will likely collect data this way as well.

29. The operative part of this warning must necessarily be seen as affecting, among other things, mobile devices, as these are in many cases part of the information systems regulated by the Cyber Security Act or the scope of their information security management. Such devices access the core assets that make up the regulated systems and a breach of their security leads to a direct threat to the security of the regulated systems and to a threat to the proper provision of the service for which those systems were placed under regulation. Furthermore, however, even those devices that are not part of regulated systems or the scope of their information security management, but which are used by strategically important persons in organisations managing or operating regulated systems, may be the target of activities consisting of the collection of sensitive information about such persons and the subsequent misuse of this information, for example, for blackmail or other forms of advancing the interests of attackers. Depending on the nature and method of use of a particular device and the nature and sensitivity of the information and data to which the device has access, the Agency therefore recommends that adequate security measures be taken to eliminate the threat to which this warning draws attention.

30. The Agency evaluates the threat level as high, i.e. in accordance with the threat assessment scale contained in Annex 2 to the Cyber Security Decree as likely to very likely. The threat level is primarily due to the combination of the problematic collection of sensitive and very easily exploitable user information and data, the low level of security and the legal environment in which DeepSeek operates and is bound by. Further, it cannot be ignored that the problematic nature of the language model has been pointed out by domestic and foreign partners, and many countries have already taken preventive measures against the Affected Products.

31. Furthermore, the Agency recommends that all natural persons whose data could be the target of foreign intelligence activities (persons of interest, i.e. persons who are, for example, in high political, public or decision-making positions) consider restricting or completely prohibiting the use of the Affected Products of DeepSeek , as set out in the statement of this warning.

32. The Agency recommends the general public pay attention to what access the Affected Products of DeepSeek request, what data they collect and how they handle it. The Agency generally recommends that only apps that the user trusts are installed and used.

33. Since the Agency's task pursuant to Section 22(j) of the Cyber Security Act is to ensure prevention in the area of cyber security, which also includes providing information on identified threats in the area of cyber security, and based on all of the above-mentioned information, which, according to the Agency, proves that the Affected Products of DeepSeek pose a security risk to the Czech Republic to the extent set out in the operative part of this warning, and as it is not sufficient to inform the public through the Agency's normal preventive activities, the Agency proceeded to issue this warning. The Agency's authority to issue this warning is provided by Section 22(b) of the Cyber Security Act.

34. Finally, the Agency points out that in accordance with Section 4(4) of the Cyber Security Act, the bodies and persons referred to in Section 3(c) to (f) of the Cyber Security Act are obliged to take into account the requirements resulting from security measures when selecting a supplier for their information or communication system and include these requirements in the contract they conclude with the supplier. Taking into account the requirements resulting from the security measures pursuant to the first sentence to the extent necessary to comply with the duties pursuant to the Cyber Security Act cannot be considered an unlawful restriction on competition or an unjustified barrier to competition.

Ing. Lukáš Kintr
Director
National Cyber and Information Security Agency