On approval of the Rules for the functioning of the program of interaction with information security researchers

Unofficial translation

Order of the Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan dated April 1, 2024 № 185/НҚ. Registered with the Ministry of Justice of the Republic of Kazakhstan on April 2, 2024 № 34211

Unofficial translation

In accordance with subparagraph 20-4) of Article 7-1 of the Law of the Republic of Kazakhstan "On Informatization" **I HEREBY ORDER**:

1. To approve the attached Rules for the functioning of the program of interaction with information security researchers.

2. The Information Security Committee of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan in accordance with the procedure established by law, shall ensure:

1) state registration of this order with the Ministry of Justice of the Republic of Kazakhstan;

2) placement of this order on the Internet resource of the Ministry of Digital Development , Innovations and Aerospace Industry of the Republic of Kazakhstan;

3) within ten working days after the state registration of this order with the Ministry of Justice of the Republic of Kazakhstan, submission to the Legal Department of the Ministry of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan of information on the implementation of the measures provided for in subparagraphs 1) and 2) of this paragraph.

3. Control over the execution of this order shall be assigned to the supervising Vice Minister of Digital Development, Innovation and Aerospace Industry of the Republic of Kazakhstan.

4. This order shall come into effect upon expiration of sixty calendar days from the date of its first official publication.

Minister of Digital Development, Innovations
and Airspace Industry
of the Republic of Kazakhstan

B. Mussin

"AGREED"
National Security Committee
of the Republic of Kazakhstan

Approved by the order of the Minister of
Digital Development, Innovations and
Airspace Industry

of the Republic of Kazakhstan
dated April 1, 2024
№ 185/НҚ

Rules for the functioning of the program of interaction with information security researchers
Chapter 1. General provisions

1. These Rules for the functioning of the program of interaction with information security researchers (hereinafter referred to as the Rules) have been developed in accordance with subparagraph 20-4) of Article 7-1 of the Law of the Republic of Kazakhstan "On Informatization" (hereinafter – the Law) and shall determine the procedure for the functioning of the program of interaction with information security researchers on objects of information technology of state bodies (hereinafter – PI with ISR on OIT of SB).

2. the following basic concepts are used in these Rules:

1) informatization object (hereinafter – IO) – electronic information resources, software, Internet resource and information and communication infrastructure;

2) owner of informatization objects - a subject to whom the owner of informatization objects has granted the rights of possession and use of informatization objects within the limits and in accordance with the procedure defined by law or agreement;

3) information security researcher (hereinafter - IS researcher) - a specialist in the field of information security and (or) information and communication technologies, registered in the program of interaction with information security researchers, who examines information objects connected to the program of interaction with information security researchers to identify vulnerabilities;

4) program of interaction with information security researchers (hereinafter - ISR) - an informatization object intended for registration of information security researchers, registration of identified vulnerabilities, as well as for ensuring interaction of information security researchers with informatization objects;

5) authorized body in the field of information security (hereinafter - authorized body) - a central executive body that carries out management and inter-sectoral coordination in the field of information security provision;

6) state technical service - a joint stock company established by the decision of the Government of the Republic of Kazakhstan;

7) operator of the program of interaction with information security researchers on the objects of informatization of state bodies (hereinafter - operator) - the State Operational Center of Information Security, ensuring the functioning of the program of interaction on the objects of informatization of state bodies (hereinafter - IO of SB);

8) vulnerability - a flaw of an informatization object, the use of which may lead to violation of integrity and (or) confidentiality and (or) availability of the informatization object
;

9) vulnerability report (hereinafter - report) - information on vulnerability in the informatization object identified by IS researcher;

10) token - a unique string value.

Chapter 2. Procedure for the functioning of the program of interaction with information security researchers по объектам информатизации государственных органов

3. Tasks and functions of the State Operational Center for Information Security as an operator, in accordance with subparagraph 6) of paragraph 1 of Article 7-8, subparagraph 3) of paragraph 1 of Article 7-4 and subparagraph 15) of paragraph 1 of Article 14 of the Law shall be implemented by the state technical service (Joint Stock Company "State Technical Service", hereinafter – JSC "STS"), which ensures the functioning of PI with ISR on OIT of SB on its own information and communication infrastructure.

4. The functioning of PI with ISR on OIT of SB shall be ensured on the basis of contractual relations between the National Security Committee of the Republic of Kazakhstan (hereinafter referred to as the NSC RK) and JSC "STS.

5. The authorized body for formation of the list of IO of SB to be connected to the PI with ISR on OIT of SB shall send a request to the owners or holders of IO of SB to provide information on IO of SB having access to the Internet (hereinafter referred to as the request).

6. Owners or proprietors of IO of SB shall send to the Authorized Body information on IO of SB having access to the Internet in the form of names of IO of SB and terms of search for vulnerabilities in it within 10 (ten) working days from the date of receipt of the request.

7. Based on the information provided by the owners or holders of IO of SB, the Authorized Body shall form a list of IO of SB to be connected to PI with ISR on OIT of SB and the timeframe for searching for vulnerabilities in IO of SB (hereinafter - the list) within 10 (ten) working days.

8. The Authorized Body shall send the list to the operator within 3 (three) working days from the date of formation of the list.

9. The Operator shall notify the owners or holders of IO of SB according to the list about the need to connect to PI with ISR on OIT of SB (hereinafter - notification about connection) within 3 (three) working days from the date of receipt of the list.

10. Owners or proprietors of IO of SB shall be obliged to take measures to ensure that OIs are connected to PIs with ISR on OIT of SB, except for OIs without Internet access in accordance with subparagraph 1) ща paragraph 2-1 of Article 54 of the Law.

11. Owners or proprietors of IO of SB, for connection to PI with ISR on OIT of SB, within 10 (ten) business days from the date of receipt of the notification of connection, shall develop and approve the research procedure, which defines the boundaries of the IO of SB research, providing for the minimum scope of testing, as well as the levels of criticality of vulnerabilities, the list of vulnerabilities that are not accepted for consideration, as well as actions that are not allowed with respect to the IO of SB when searching for vulnerabilities.

12. Owners or proprietors of IO of SB shall send the research procedure to the operator within 2 (two) business days from the date of its approval.

The Operator shall place the study order in the PI with ISR on OIT of SB within 2 (two) working days from the date of its receipt.

13. The IS researcher shall register in the PI with ISR on OIT of SB and receive a token with which the IS researcher shall mark the traffic, request, parameter when searching for vulnerabilities in the IO of SB.

14. The IS researcher may not disclose the token to third parties or use third party tokens.

15. When examining the IO of SB for vulnerabilities, an IS researcher may not:

1) investigate IP addresses and domain names not specified in the PI with ISR on OIT of SB;

2) use tools for automatic scanning of the OIT of SB except as agreed by the owner or proprietor of the IO of SB;

3) attempt to exploit a vulnerability, except for the minimum amount of testing specified in the research order and necessary to prove the existence of the vulnerability or to identify an indicator associated with the vulnerability;

4) intentionally access the contents of any messages, data, or information transmitted or stored in the IO of SB, unless the information is directly related to the vulnerability and access is necessary to prove the existence of the vulnerability;

5) offload, store, disclose, transmit, modify, delete any data or information accessed during the course of the investigation;

6) disclose any information about the vulnerability of the IO of SB or the content of information obtained through exploitation of the vulnerability, except for the case of obtaining written authorization from the owner or proprietor of the IO of SB;

7) attempt to gain access to IO of SB user accounts, unless they have been provided to the IS researcher by the owner or proprietor of the IO of SB for the purpose of the research;

8) use methods of physical intervention in the IO of SB;

9) use social engineering methods against employees or contractors of the owner or proprietor of the IO of SB or the operator of the IO of SB.

16. If exploitation of the detected vulnerability may result in compromising the integrity and availability of the IO of SB, the IS researcher shall refrain from actions to exploit this vulnerability and shall specify in the report the data necessary to verify the found vulnerability.

17. The IS researcher shall send the report to the operator via PI with ISR on OIT of SB in accordance with the form posted in PI with ISR on OIT of SB.

18. Within 15 (fifteen) working days from the date of receipt of the report, the Operator shall verify its accuracy and prepare a conclusion on the presence or absence of vulnerability in the IO of SB.

19. When verifying the report, the Operator shall, if necessary, request from the IS researcher additional information confirming the presence of vulnerability in the IO of SB.

20. In case of failure to confirm the reliability of the report, the Operator shall, within 5 (five) working days after verification of the report, send to the IS researcher a conclusion on the absence of vulnerability in the IO of SB by means of PI with ISR on OIT of SB.

21. If the report is confirmed to be accurate, the operator shall, within five (5) business days after verification of the report through PI with ISR on OIT of SB:

1) notifies the owner or holder of the IO of SB about the presence of vulnerability in the IO of SB (hereinafter - vulnerability notification) and sends him the report;

2) notifies the authorized body about the presence of vulnerability in the IO of SB;

3) inform the IS researcher about the results of the audit.

22. The operator shall not forward the report to the owner or holder of the IO of SB and to the authorized body if:

1) failure of the operator to confirm the reliability of the report;

2) the operator confirms the existence of an identical vulnerability before the report is sent by the IS researcher.

23. The owner or holder of IO of SB is obliged to take measures to ensure elimination of identified vulnerabilities registered in PI with ISR on OIT of SB in accordance with subparagraph 2) of paragraph 2-1 of Article 54 of the Law.

24. The owner or holder of the IO of SB within fifteen (15) business days of receiving notification of the vulnerability shall:

1) eliminates the vulnerability and sends information about its elimination to the operator through PI with ISR on OIT of SB;

2) if it is impossible to eliminate the vulnerability, sends to the operator and the authorized body via PI with ISR on OIT of SB information on failure to eliminate the vulnerability in IO of SB, which contains:

justification of non-elimination of vulnerability and nature of required changes in IO of SB;

measures aimed at minimizing the risks of exploitation of the identified vulnerability;

timeframes for eliminating the vulnerability, not exceeding 6 (six) months from the date of first detection.

25. The Operator after expiration of the period of vulnerability elimination defined in paragraph 24 of these Rules shall check the IO of SB for elimination of vulnerability within 5 (five) working days.

If the owner or holder of the IO of SB fails to eliminate the vulnerability in the IO of SB, the operator shall notify the authorized body and the NSC of the Republic of Kazakhstan by means of PI with ISR on OIT of SB within 1 (one) working day after the expiration of the check period.

26. In case of violation by IS researcher of paragraphs 13, 14, 15, 16 and 17 of these Rules and the research procedure, the operator shall block the IS researcher's account in PI with ISR on OIT of SB.