Data Bank of Information Security Threats

home (/) / Regulations for enabling vulnerabilities

METHODOLOGICAL DOCUMENT

REGULATIONS FOR INCLUDING INFORMATION ABOUT SOFTWARE AND SOFTWARE AND HARDWARE VULNERABILITIES IN THE DATA BANK OF INFORMATION SECURITY THREATS OF THE FSTEC OF RUSSIA

1. GENERAL PROVISIONS

1.1. These Regulations for the inclusion of information about software and hardware vulnerabilities in the database of information security threats of the FSTEC of Russia were developed in accordance with subparagraph 4 of paragraph 8 of the Regulations on the Federal Service for Technical and Export Control, approved by the Decree of the President of the Russian Federation of August 16, 2004. No. 1085, and is aimed at implementing the Regulations on the Data Bank of Information Security Threats, approved by Order No. 9 of the FSTEC of Russia dated February 16, 2015 (registered by the Ministry of Justice of Russia on April 17, 2015, reg. No. 36901).

1.2. The Regulations determine the procedure for interaction between the FAU "GNIIII PTZI FSTEC of Russia", which ensures the functioning of the database of information security threats (hereinafter referred to as the Operator), with developers and manufacturers of software and software and hardware (hereinafter referred to as manufacturers), with organizations and specialists who identify (detect) software and hardware vulnerabilities (hereinafter referred to as researchers), when including information about software and hardware software vulnerabilities (hereinafter referred to as vulnerabilities) in the database of information security threats of the FSTEC of Russia (hereinafter referred to as the Threat Data Bank).

1.3. As part of the interaction, the Operator may enter into an agreement with the manufacturer on the non-disclosure of information about vulnerabilities coming from the manufacturer, taking into account the provisions of these Regulations.

2. OBTAINING INFORMATION ABOUT VULNERABILITIES

2.1. Information about vulnerabilities can be obtained by the Operator:

upon receipt of information about vulnerabilities from manufacturers;

upon receipt of information about vulnerabilities from researchers;

when performing research on the instructions of the FSTEC of Russia.

2.2. Information about the vulnerability is sent to the Threat Data Bank through the “Feedback” section (bdu.fstec.ru) or to the email address webmaster@bdu.fstec.ru. (mailto:webmaster@bdu.fstec.ru)The vulnerability information includes the following information:

name of the vulnerability and its description;

name and version of the vulnerable software or hardware;

developer/manufacturer (vendor) of vulnerable software or hardware (if any);

error type and identifier in accordance with the general list of CWE errors;

names of operating systems and types of hardware platforms for which the vulnerability is relevant;

base vector and severity level [1] vulnerability in accordance with CVSS v.3.0;

procedure for checking vulnerability and supporting materials (RoS code, video demonstration or others);

contact information of the manufacturer (name of the organization and address of its location, position, surname, first name, patronymic (if any) of the head of the organization, name of the unit responsible for eliminating vulnerabilities, telephone number, email address) or researcher (name, email address and (or) telephone number).

2.3. Information about the vulnerability can be sent using PGP keys (/contacts/email) located in the "Feedback" section of the Threat Data Bank.

[1] In accordance with GOST R 56545 - 2015, the degree of vulnerability danger can take one of four values; critical (CVSS score – 10), high (CVSS score – 7-9.9), medium (CVSS score – 4-6.9), low (CVSS score – 0-3.9)

3. PROCESSING INFORMATION ABOUT VULNERABILITIES

3.1. Processing information about vulnerabilities received from manufacturers

3.1.1. When a manufacturer identifies a vulnerability in its software or hardware and software, it sends information about the identified vulnerability to the Threat Data Bank in accordance with paragraph 2.2 of these Regulations within 3 business days from the date of its identification.

If the manufacturer has received information about a potential vulnerability in its software (hardware) from an external source (including from researchers in accordance with paragraph 3.2.1 of these Regulations), then the information about the vulnerability is sent by the manufacturer to the Threat Data Bank after preliminary verification and assessment of the severity of this potential vulnerability. Information about the vulnerability received from the researcher is sent with the contact information of the researcher who identified the vulnerability to be taken into account when determining the researcher's rating in accordance with clause 4.3 of these Regulations (if the researcher has consent to provide such data).

The recommended period for preliminary verification and assessment of the severity of a potential vulnerability should not exceed 5 business days from the date of receipt (publication) of information about the presence of a potential vulnerability.

3.1.2. When receiving information from the manufacturer about a vulnerability or potential vulnerability, the Operator, within no more than 3 business days, checks the availability of information about it in the Threat Data Bank, as well as in other vulnerability databases and public sources, and if there is no information in them, reserves for the vulnerability (potential vulnerabilities) temporary identifier (BDU-Z-XXXX-xxxxx) of the Threat Data Bank.

Information about the reserved temporary identifier for the vulnerability (potential vulnerability) is sent to the manufacturer at the email address specified by him.

If there is information about a vulnerability (potential vulnerability) in the Threat Data Bank, the Operator informs the manufacturer about this and, if necessary, clarifies the description of the vulnerability in the Threat Data Bank. If there is information about a vulnerability (potential vulnerability) in other publicly available vulnerability databases or sources, the Operator, within 3 working days, assigns a permanent identifier to the vulnerability (BDU-XXXX xxxxx), in cooperation with the manufacturer, creates a description of the vulnerability, a sample of which is given in Appendix No. 1 to these Regulations, and places it in the Threat Data Bank.

Information about a vulnerability in software or hardware certified according to information security requirements is sent by the Operator to the central office of the FSTEC of Russia to the email address otd24@fstec.ru within 1 business day from the date of receipt to support the manufacturer's work to eliminate the vulnerability in the certified (mailto:otd24@fstec.ru) software or software or hardware.

3.1.3. The Manufacturer, in relation to the vulnerability for which the Operator has reserved a temporary identifier, develops measures to eliminate this vulnerability (for example, developing a patch, releasing a new version), or takes legal, organizational, technical measures that reduce the possibility of exploitation of the vulnerability by an intruder (hereinafter referred to as elimination measures vulnerabilities).

In relation to a potential vulnerability for which a temporary identifier has been reserved by the Operator, the manufacturer conducts research to confirm its relevance and clarify the degree of danger, after which it develops measures to eliminate the vulnerability.

In relation to a vulnerability (potential vulnerability) of a critical or high level of danger, the recommended period for developing measures to eliminate it (including confirmation of relevance) should not exceed 30 business days from the moment the vulnerability is identified by the manufacturer or data on the vulnerability is received from external sources.

For a vulnerability (potential vulnerability) of medium or low severity, the recommended period for developing measures to eliminate it (including confirmation of relevance) should not exceed 60 business days from the moment the vulnerability is identified by the manufacturer or data on vulnerabilities is received from external sources.

If, as a result of research into a potential vulnerability by the manufacturer, its relevance is not confirmed, information about this is sent to the Threat Data Bank. Upon receipt of the specified information, the operator cancels the reserved temporary identifier of the potential vulnerability and informs the manufacturer about it.

3.1.4. After developing measures to eliminate the vulnerability in accordance with paragraph 3.1.3 of these Regulations, the manufacturer sends updated information about the vulnerability for which a temporary identifier is reserved, and the composition of measures to eliminate the vulnerability to the Threat Data Bank.

The operator, upon receiving updated information about the vulnerability from the manufacturer, creates a description of the vulnerability, a sample of which is given in Appendix No. 1 to these Regulations, agrees on the description of the vulnerability with the manufacturer, and then places the description of the vulnerability in the Threat Data Bank with the assignment of a permanent identifier (BDU-XXXX-xxxxx) .

A description of a vulnerability of a critical or high level of danger is posted in the Threat Data Bank no later than 5 business days from the date of receipt of information about the vulnerability from the manufacturer.

Descriptions of vulnerabilities of medium or low severity are posted in the Threat Data Bank no later than 7 business days from the date of receipt of information about the vulnerability from the manufacturer.

3.1.5. Additional information about the vulnerability is sent by the manufacturer to the Threat Data Bank through the "Feedback" section or to the email address webmaster@bdu.fstec.ru. (mailto:webmaster@bdu.fstec.ru)Upon receipt of additional information, the operator makes changes to the description of the vulnerability within 1 business day.

3.2. Processing information about vulnerabilities received from researchers [2]

3.2.1. When a researcher identifies a vulnerability, it is recommended that information about it be sent to the manufacturer of the software or hardware in which the vulnerability was identified, so that it can be checked and corrective measures taken.

If there is no response within 5 business days, the researcher is advised to resubmit the vulnerability notification to the manufacturer.

Simultaneously with sending information about the vulnerability to the manufacturer, it can be sent to the Threat Data Bank in accordance with clause 2.2 of these Regulations.

Information about a vulnerability in software or hardware certified according to information security requirements is additionally sent to the central office of the FSTEC of Russia to the email address otd24-bdu@fstec.ru to (mailto:otd24-bdu@fstec.ru) support the manufacturer's work to eliminate the vulnerability in the certified software or hardware.

3.2.2. If it is impossible to obtain contact information for the manufacturer's technical support service, as well as if the manufacturer fails to take measures to eliminate the vulnerability, the researcher is recommended to send information about the vulnerability to the Threat Data Bank in accordance with clause 2.2 of these Regulations.

In this case, failure to take measures to eliminate the vulnerability is considered:

failure to respond within 5 business days to a repeated notification of a vulnerability or to another subsequent request sent to the manufacturer;

refusal to interact to confirm or eliminate a vulnerability, expressed verbally or in writing;

absence of measures to eliminate the vulnerability published in the Threat Data Bank within 60 working days from the date of provision of information by the researcher.

3.2.3. Upon receipt of information about a vulnerability from a researcher, the Operator, within no more than 3 business days for a vulnerability of a critical or high level of danger and 5 business days for a vulnerability of a medium or low level of danger, checks the availability of information about the identified vulnerability in the Threat Data Bank, as well as in other publicly available vulnerability databases and sources.

If there is information about an identified vulnerability in the Threat Data Bank, the Operator informs the researcher about this and, if necessary, clarifies the description of the vulnerability in the Threat Data Bank. If information about the vulnerability is available in other publicly available vulnerability databases or sources, the Operator informs the researcher about this, assigns a permanent identifier to the vulnerability (BDU-XXXX-xxxxx), generates a description of the vulnerability and places it in the Threat Data Bank.

Information about a vulnerability in software or hardware certified according to information security requirements is sent by the Operator to the central office of the FSTEC of Russia to the email address otd24-bdu@fstec.ru within 1 business day from the date of receipt to support the manufacturer's work to eliminate the vulnerability in the (mailto:otd24-bdu@fstec.ru) certified software or hardware software.

3.2.4. If there is no information about the vulnerability in the Threat Data Bank or in other publicly available vulnerability databases (sources of information), the Operator, if contact information is available, sends a notification about the vulnerability to the manufacturer's technical support service and requests the contact information of the manufacturer's persons who need to provide full information about the identified vulnerability.

If there is no response within 5 business days, the Operator re-sends the vulnerability notification to the manufacturer.

Upon receipt of a response, the Operator sends to the manufacturer the available information about the potential vulnerability for verification, as well as information about the researcher who identified the vulnerability (if the researcher has consent to provide information).

If necessary, the Operator will organize interaction between the manufacturer and the researcher who identified the vulnerability in order to confirm the presence of the vulnerability and develop measures to eliminate it.

3.2.5. When receiving information about a vulnerability from the Operator, the Manufacturer checks it and, if the presence of such a vulnerability is confirmed, sends updated information to the Operator.

3.2.6. Upon receipt of confirmation of the vulnerability from the manufacturer, the operator reserves a temporary identifier for the vulnerability (BDU-Z XXXX-xxxxx), which he informs the manufacturer about.

Further interaction between the Operator and the manufacturer is carried out in accordance with paragraphs 3.1.2 - 3.1.5 of these Regulations.

3.2.7. If it is impossible to obtain contact information for the manufacturer's technical support service, as well as if the manufacturer fails to take measures to eliminate the vulnerability, the Operator conducts independent research to confirm the presence of a vulnerability in the software or firmware.

In this case, failure to take measures to eliminate the vulnerability is considered:

failure to respond within 5 business days to a repeated notification of a vulnerability or to another subsequent request sent by the Operator;

refusal to interact with the Operator in accordance with clauses 3.1.2 - 3.1.5 of these Regulations.

The period for the Operator to conduct vulnerability research should not exceed 60 business days from the date of receipt of information from the researcher. Depending on the complexity of the vulnerable software or hardware and software, this period may be extended by agreement with the FSTEC of Russia.

Research may be conducted in collaboration with the researcher who submitted the vulnerability.

To conduct research, the Operator, on the basis of an agreement, may involve expert organizations that are participants in maintaining the Threat Data Bank (organizations participating in the Threat Data Bank). [3] Information about a vulnerability being researched by an organization participating in the Threat Data Bank is not subject to disclosure.

3.2.8. Upon confirmation, based on the results of research conducted in accordance with clause 3.2.7 of these Regulations, the presence of a vulnerability in software or hardware and software, the Operator assigns a permanent identifier to the vulnerability, in interaction with the researcher who sent information about the vulnerability, creates a description of the vulnerability, a sample of which is given in Appendix No. 1 to these Regulations, and places it in the Threat Data Bank.

[2] Information about vulnerabilities identified by researchers based on customer assignments can be submitted to the Threat Data Bank only in agreement with the relevant customers.

[3] The list of organizations that are participants in the Threat Data Bank is posted in the “Participants/Organizations” section of the website bdu.fstec.ru.

4. DISCLOSURE OF INFORMATION ABOUT VULNERABILITIES

4.1. Disclosure of information about the vulnerability is carried out by the Operator posting a description of the vulnerability in the Threat Data Bank.

4.2. Disclosure of information about a vulnerability in the Threat Data Bank is carried out if:

information about the vulnerability is published in other publicly available vulnerability databases or sources;

information about the vulnerability and measures to eliminate it was received from the manufacturer in accordance with these Regulations;

the manufacturer does not take measures to eliminate the vulnerability in accordance with this Regulation;

There are no contact details for the manufacturer or its technical support service.

4.3. The operator, based on information about vulnerabilities provided by researchers, maintains a rating of researchers (“honor board”) and places it on the website of the Threat Data Bank (if the researchers have consent to post such information). The rating is determined in accordance with Appendix No. 2 to these Regulations by calculating the points assigned to the researcher for the information provided about previously unknown vulnerabilities and published in the Threat Data Bank.

4.4. Researchers who have identified a vulnerability are not recommended to disclose information about vulnerabilities without approval from the manufacturer or Operator.

Appendix No. 1
to the Regulations for the inclusion of information
on software
and hardware software vulnerabilities
in the database of
information security threats of the FSTEC of Russia

Description of the vulnerability for placement in the Threat Data Bank

BDU: XXXX-xxxxx: Vulnerability name

Description of the vulnerability	
Name of the vulnerable software	
Vulnerable software version	
Manufacturer/developer (vendor)	
Name of the operating system and type of hardware platform for which the vulnerability is relevant	
Error type (id)	
Vulnerability class	
Date of vulnerability discovery	
Basic vulnerability vector	
Vulnerability severity level	
Possible mitigation measures	

Vulnerability status	
The presence of an "exploit"	
Method of operation	
Remedy	
Vulnerability Remediation Information	
Sources that published information about the vulnerability	
Vulnerability identifiers in other description systems	
Other information about the vulnerability	

Appendix No. 2
to the Regulations for the inclusion of information
on software
and hardware software vulnerabilities
in the database of
information security threats of the FSTEC of Russia

Determining the rating of researchers who provided information about vulnerabilities to the Threat Data Bank

The researcher receives rating points for providing information about vulnerabilities to the Security Threat Data Bank if the following conditions are met:

1) information about the vulnerability has not been previously published in the Threat Data Bank or other publicly available sources;

2) the researcher provided information about the vulnerability and the researcher's contact information in accordance with the Regulations for handling information about software and hardware vulnerabilities in the Data Bank of Information Security Threats of the FSTEC of Russia.

The number of rating points for an identified vulnerability is determined by the following formula:

$A = (T + P + R)* C$, where

T – indicator characterizing the object of research (the type of software with the maximum value is selected);

P – indicator characterizing the vulnerability verification algorithm and supporting materials;

R – indicator characterizing the level of danger of vulnerability;

C is an indicator characterizing the amount of affected software.

A researcher's overall rating is determined by simply summing up all the rating points a researcher has received for information about vulnerabilities that have been submitted to the Threat Data Bank.

Indicator values when determining the rating:

Criteria	Values	Points
Indicator characterizing the object of research (T)	Embedded software (firmware), telecommunications equipment software, information security software	10
	System-wide software (including virtualization software), software for automated process control systems	7
	Application software (including database management systems)	5
Indicator characterizing the vulnerability verification algorithm and supporting materials (P)	PoC developed or action algorithm presented	3
	Video confirmation provided	2
	Other methods	1
Indicator characterizing the level of vulnerability danger (R)	Defined according to CVSS v.3.0 evaluation: critical (10) high (7-9.9); average (4-6.9); low (0-3.9)	10 7 3 1
Indicator of the number of software affected by the vulnerability (C)	The vulnerability affects several types of software (multiple vulnerability)	1.5
	The vulnerability is relevant only for one type of software	1.0

If the researcher additionally provides a description of the vulnerability in the OVAL language, then an additional 2 points are added to the total number of rating points calculated using the above formula.

The maximum possible number of rating points for one vulnerability is **36.5** .

The minimum possible number of rating points for one vulnerability is **7** .

LAST CHANGES

10/04/2023
Protected information disclosure vulnerability in the WebKitGTK and WPE WebKit web page rendering modules, which could allow an attacker to disclose protected information (/vul/2023-06302)

10/04/2023
A vulnerability in the Application Quality of Experience (AppQoE) and Unified Threat Defense (UTD) components of the Cisco IOS XE operating system that allows an attacker to cause a denial of service (/vul/2023-06301)

10/04/2023
A vulnerability in the web interface of the Cisco IOS XE operating system allows an attacker to execute arbitrary commands (/vul/2023-06300)

10/04/2023
A vulnerability in the Extensions component of the Google Chrome browser that allows an attacker to execute arbitrary code (/vul/2023-06299)

10/04/2023
A vulnerability in the Passwords component of the Google Chrome browser that allows an attacker to execute arbitrary code (/vul/2023-06298)

Threats: **222** Vulnerabilities: **50586** Last update: **10/04/2023**

(https://metrika.yandex.ru/stat/?id=28243701&from=informer)