Cybozu Bug Bounty Program Rulebook

0. Preface

The Cybozu Bug Bounty Program (hereafter called "this program") is a system intended to early discover and remove zero-day vulnerabilities that might exist in services provided by Cybozu. Under this program, people who discover vulnerabilities and report them to us (hereafter called "reporters") will be paid a reward as a token of our gratitude for cooperating to help us improve the quality of our services.

1. Services That Are Applicable for Testing

To learn which services are applicable for testing under this program, see the Cybozu Bug Bounty Program page (https://cybozu.co.jp/products/bug-bounty/). The latest versions of each service are the targets of testing under this program. To learn the details about our services, see the Web site of each product.

2. Terms and Conditions on Reporting

Those who fulfill the below conditions may receive a reward for reporting vulnerability information under this program.

- You are not an employee of Cybozu Inc. or its subsidiary companies.
- You can communicate with Cy-PSIRT in Japanese or English.
- You agree with the Terms and Conditions for Cybozu Bug Bounty Program.

You can see the Terms and Conditions for Cybozu Bug Bounty Program at the following URL:
https://cybozu.co.jp/products/bug-bounty/pdf/Terms_and_Conditions_for_Cybozu_Bug%20Bounty_Program.pdf

3. Communication

3.1 Contact Us

This program is managed by Cy-PSIRT under Cybozu, Inc. All inquiries regarding this program must be made by e-mail or by using the Web form. Inquiries made by other methods will not be answered.

Web Form:
https://www.cybozu.com/jp/support/security.html?

E-mail:
productsecurity@cybozu.co.jp

3.2 Service Time

Our service time is between 9:00 (JST) - 17:30 (JST) on weekdays.

3.3 PGP Key

When reporters contact Cy-PSIRT, they can use a PGP key. The public key information is available at the following: https://www.cybozu.com/jp/features/management/Cy-PSIRT.asc

4. Cybozu Vulnerability Information Handling Policy

All vulnerability information that is reported to Cybozu will be received and handled in accordance with Cybozu's "Vulnerability Information Handling Policy". The Vulnerability Information Handling Policy defines how we will handle and publicize any vulnerabilities that are discovered in the products and services that Cybozu offers. For details, see the following Japanese Web site: https://cybozu.co.jp/company/security-policy/

5. Evaluation Process for Vulnerability Information

5.1 Evaluation Process

A vulnerability reported from a reporter to Cy-PSIRT is evaluated by using the following process:

1. We assign a "response number" and communicate it to the reporter.
2. We evaluate the vulnerability based on the reported information.
3. We contact the reporter with the evaluation results.

   - When the evaluation determines that the reported vulnerability is a qualifying vulnerability, we will communicate the results to the reporter.
   - When the evaluation determines that the reported vulnerability is not a qualifying vulnerability, we will communicate the results to the reporter.
   - When we determine that additional information is necessary, we will contact the reporter again.

4. The reporter contacts Cy-PSIRT with "response completed", and then the evaluation process is completed.
   * At this point, the evaluation and the payment amount may vary.
5. When we contact you about payment, we will again inform you about the evaluation and the payment amount.
   * At that point, you will confirm the payment amount, and the payment amount will not be modified afterward.

5.2 Order in Which Inquiries to Be Accepted

Received inquiries are accepted in the order of the time stamp on the received e-mail.

5.3 Time for Acceptance

Generally, received inquiries are accepted within two business days.

5.4 Order in Which Vulnerabilities to Be Evaluated

Generally, vulnerabilities are evaluated in the order of the response number. However, the evaluation order may be changed due to the vulnerability report status and so on.

6. Rewards

6.1 Formula for Calculating the Payment Amount

The amount of the reward is determined according to the following rules:

No	Summary	Case	Calculation method
1	Has the vulnerability been conclusively identified?	Yes	Formulas 2 to 8 are applied.
		Yes (RCE)	1 million yen (Flat rate). Formulas 6 to 8 are applied.
		Revocation of identification after full completion	20,000 yen (Flat rate). Formulas 6 to 8 are applied. * For reports worth less than 20,000 yen, the reporter will earn the original amount.
		No	No payment.
2	Base amount	Product	CVSSv3 base score
		Homepage	20,000 yen (Flat rate). Formulas 6 to 8 are applied.
3	Coefficients by CVSSv3 base score	0.0 to 6.9	x 10,000 yen
		7.0 to 8.9	x 30,000 yen
		9.0 to 10.0	x 50,000 yen
4	Coefficients by vulnerability type	SQL injection if the CVSS v3 base score is less than or equal to 6.9	x 3
		Others	x 1
5	Coefficients by product	kintone cybozu.com Administration	x 5
		Garoon Office Mailwise	x 2 * Optional products are not included.
		None of the above	x 1

6	Pre-identification report	First reporter	x 1
		Subsequent reporters	x 0.2
7	Maximum amount	-	2 million yen * Includes cases such as when we have received reports for the same type of vulnerability in different products.
8	Additional payments by payee	Reporter	x 1
		Contribution	x 2

6.2 Detailed Rules on Earing Rewards

No	Case	Reward	Rules
1	As a result of investigation, multiple qualifying vulnerabilities are recognized.	Yes	If Cybozu recognizes multiple qualifying vulnerabilities from a vulnerability report, the reporter earns a reward for each vulnerability. In such a case, the maximum total amount of the rewards is 2,000,000 yen.
2	Identical or similar vulnerabilities are reported.	No	When identical or similar vulnerabilities are reported for the same product, they are handled as a single vulnerability. The reporter earns a reward based on the evaluation of the single vulnerability.

6.2.1 Examples of Identical Vulnerabilities with the Same Root Cause

- Both input from a parameter and input from a hash object expose vulnerabilities.
- Multiple unescaped parameters of a method expose vulnerabilities.
- Multiple Web sites hosted on the same server expose vulnerabilities caused by the configuration of the environment.

This rule does not apply if identical vulnerabilities with the same root cause are exposed in different products.

6.2.2 Examples of Similar Vulnerabilities

- Different processes that use the same logic expose vulnerabilities in several places.
- The different types of logic that use the same parameter, DOM attribute, or something like that expose vulnerabilities.

This rule does not apply if similar vulnerabilities are exposed in different products.

No	Case	Reward	Rules
3	Multiple vulnerability reports are received at the same time.	Yes	When a vulnerability is being evaluated and another reporter reports a vulnerability that is similar or identical to the first vulnerability, one of the vulnerabilities can be recognized as a qualifying vulnerability. The reporter of the qualifying vulnerability earns the full amount for the reward, whereas others earn 20% of the reward.
4	A known vulnerability is reported.	No	A reporter cannot earn a reward when the reported vulnerability is a known vulnerability that was already reported by another reporter. * Definition of a known vulnerability A qualifying vulnerability that is recognized by Cybozu but that is not yet public. We will not pay a reward, however thanks will be given on the following Japanese page: https://cybozu.co.jp/products/bug-bounty/specialthanks/
5	An add-on to a vulnerability from another reporter is reported.	Yes	A reporter of a vulnerability that is similar to one from a different reporter earns a reward, unless the vulnerability is a known vulnerability.
6	A publicized vulnerability is reported.	No	If a reported vulnerability is a publicized vulnerability, the reporter cannot earn a reward.
7	A vulnerability is reported for an environment that is not supported.	No	If a reported vulnerability is reproduced in a browser that is not supported, the reporter cannot earn a reward. For information about supported browsers, see the Web site of each product.
8	It is decided that a reported vulnerability will not be fixed in Cybozu products.	Yes	If it is decided that a qualifying vulnerability will not be fixed, the reporter earns a reward based on the evaluation results of the qualifying vulnerability when the decision is made.
9	A vulnerability in WordPress is reported.	Yes	When a vulnerability is publicized from WordPress, two weeks are allowed for Cybozu to analyze the impact and address the vulnerability. After that, the reported vulnerability is recognized as a qualifying vulnerability only when the reported vulnerability is an unknown vulnerability and has impact. The reporter earns a reward based on the evaluation results of the qualifying vulnerability.
10	A vulnerability is reported for a third party product used within our products.	Yes	The system is updated as necessary based on the severity. After the update, the reported vulnerability is recognized as a qualifying vulnerability only when the reported vulnerability is an unknown vulnerability and has impact. The reporter earns a reward based on the evaluation results of the qualifying vulnerability.

6.3 Changes to Evaluation Results After the Recognition

No	Case	Reward	Rules
11	Once a vulnerability was recognized as a qualifying vulnerability, the score of the vulnerability is changed.	Yes	If the evaluation results of a vulnerability is changed as a result of the investigation after the vulnerability was recognized as a qualifying vulnerability, the reporter earns a reward based on the evaluation results after the change.
12	Once a vulnerability was recognized as a qualifying vulnerability, the vulnerability is determined not to be a qualifying vulnerability as a result of the investigation.	Yes	If a vulnerability is determined not to be a qualifying vulnerability as a result of the investigation after the vulnerability was recognized as a qualifying vulnerability, the reporter earns 20,000 yen for any case. However, when the original reward amount is less than 20,000 yen, the reporter earns the original amount.
13	It is decided that a reported vulnerability will not be fixed in Cybozu products.	Yes	If it is decided that a qualifying vulnerability will not be fixed, the reporter earns a reward based on the evaluation results of the qualifying vulnerability when the decision is made.

6.4 Delivery of Rewards

If a vulnerability reported by a reporter fulfills the below requirements, we will transfer the reward in cash at the end of the following month.

- Cybozu released the vulnerability information to the general public.
- Cybozu recognized the vulnerability as a qualifying vulnerability, and then six months passed without publication of the vulnerability information.

Reporters must send their bank details to Cy-PSIRT. Note that we cannot transfer money to corporate accounts.

6.5 Donating Rewards

Reporters can donate earned rewards to an OSS community selected by Cybozu, instead of claiming the reward. If a reporter chooses to donate their reward, Cybozu also will donate the same amount as their reward to the OSS community. However, you must accept each reward in its entirety or donate it. You cannot split the reward between yourself and a donation.

6.5.1 Donation Recipients Selected by Cybozu

- Apache Software Foundation
- Linux Foundation
- OWASP Local Chapter in Japan

If a reporter does not specify a recipient, we make the donation to the Apache Software Foundation.

6.5.2 Donation Details

Once we have been contacted by a reporter saying that they wish to donate, Cybozu makes the donation within two months to the organization of the reporter's choice. The donation is made in the name of "Cybozu, Inc." Once the donation has been made, Cybozu notifies the reporter of the completion. We cannot accept requests such as issuing documents intended to be used for tax breaks, and so on. It is confirmed that the recipients listed above cannot enable a reporter to receive a tax break when the reporter lives in Japan.

6.6 Taxation in Japan

If the reward amount earned by the reporter exceeds a certain amount, the reporter has a duty to submit a final income tax return on their own. For details on final income tax returns, on the National Tax Agency's Web site as found below, see "1-12 Who Must File a Final Return" and "3-2 #8 Occasional Income" (page 32).
http://www.nta.go.jp/taxes/shiraberu/taxanswer/shotoku/1900.htm
http://www.nta.go.jp/taxes/shiraberu/taxanswer/shotoku/1490.htm
The reporter may not be qualified as a dependent for tax calculations, even if the reporter does not have other income. However, this does not influence the dependent status for health insurance calculations. For details on exemptions for dependents, on the National Tax Agency's Web site as found below, see "3-3 #13 Exemption for dependents" (page 45).
https://www.nta.go.jp/taxes/shiraberu/taxanswer/shotoku/1180.htm

7. Testing Environment

See the Bug Bounty Testing Environment Program page.

https://cybozu.co.jp/products/bug-bounty/#TestingEnvironmentProgram

Update history

Jun. 19, 2014	First edition released.
Jun. 25, 2014	Removed Cybozu Live from the list of applicable services of the bounty program.
Jul. 17, 2014	Fixed typographical errors. Changed the multiplication sign in the reward formula. Added the details of applicable Web sites.
Feb. 02, 2015	Amended the time frame for the program. Changed the list of applicable Web sites. Removed detailed information about the PGP public key. Fixed typographical errors. Changed the version of Garoon. Added description about giving thanks for reporters.
Jun. 16, 2015	Added rules about donations. Added Cybozu Live and cybozu.com operational base to the list of applicable services.
Feb. 01, 2016	Updated the payment rules for rewards. Added サイボウズ office 新着通知 (Cybozu Office New Notifications)*, Cybozu Live Timeline, Cybozu CDN, and Cybozu Desktop to the list of applicable services. Removed redundant parts in the document. * Japanese version only
Jan. 15, 2017	Removed the year. Removed "Cybozu Online Service" from the list of applicable products. Changed the time frame for the program to the year 2017. Reflected the change in the URL to the Vulnerability Information Handling Policy.
Jul. 07, 2017	Unified this document with the guidelines, and appended insufficient information.
Apr. 09, 2018	Changed the Terms and Conditions on Reporting. Changed the Response time.Increased the maximum amount of rewards. Updated tax explanation.
Aug. 10, 2018	Updated the evaluation processes. Added the formura for calculating the payment amounts.