TSRC Evaluation and Rewards Terms

Written By	**Tencent Security Response Center**
Version	**2.1**
Last Update Date	**15/10/2015**

The Scope of Application

The terms applies to all intelligence received by TSRC.

Implementation Date

This document is implemented since the date of publication.

Contents

Basic Principles

1) Tencent attaches great importance to the security of its products and businesses. We promise that every report is taken care of and given timely replies by specially assigned team.

2) Tencent appreciates responsible disclosure and handling of security vulnerabilities. We promise that every user who abides by the spirit of white hat, protects the interests of users, and helps Tencent enhance the security quality, will get sincere thanks and feedbacks from TSRC.

3) Tencent opposes and condemns all hacker activities that exploit security vulnerabilities to damage users' interests under the pretext of vulnerability testing, including but not limited to using vulnerabilities to steal user privacy, data and virtual property, invading business systems, maliciously spreading vulnerabilities, etc. .

4) Tencent opposes and condemns all activities that exploit security vulnerabilities to threaten users and attack competitors.

5) Tencent believes that the handling of every security vulnerability and the progress of the entire industry are inseparable from the cooperation of all parties. We hope that companies, security organizations and security

researchers can support the responsible disclosure of vulnerabilities to build a more safe and healthy Internet together.

Handling Process of Threat Intelligence

Pre-reporting

Threat intelligence reporters authorize TSRC to set up their accounts.

Reporting

Reporters login in TSRC to report security vulnerabilities. (Status: pending review)

Processing

1) Tencent Security Response Center (hereinafter referred to TSRC) will begin to assess the security issues reported within one working day. (Status: Under review)

2) Within three working days, TSRC will draw a conclusion and score (Status: ignored / confirmed). TSRC may contact the reporter for further information if necessary.

Fixing

1) The business departments fix the security problems and launch the new version (Status: fixed). The repair time depends on the severity of the problem and the difficulty of the repair. In general, serious and high-risk issues within 24 hours, medium-risk issues within three working days, low-risk issues within seven

working days. Due to the release restrictions, the repair time of client security issues varies, depending on the actual situation.

2) The reporters of security vulnerabilities review whether the security issues are fixed. (Status: Reviewed / Objected)

Completing

1) In the first week of each month, TSRC will post a security announcement of last month, and publicly give thanks to the reporters. Some emergency security announcements will separately post if necessary.

2) The reporters can use Points to redeem SecCoins, and exchange cash or gifts in TSRC′ virtual market with SecCoins. Besides, there will be rewards and offline activities for reporters from time to time.

3) With the permission of the threat intelligence reporters, TSRC will select some representative security issues to analyze and publish articles on TSRC official website from time to time.

Vulnerability Assessment Standard

Tencent threat intelligence mainly includes three parts: vulnerabilities of Tencent applications, vulnerabilities of general software and security intelligence.

Vulnerability Assessment Standard for Tencent Applications

According to the severity, a reported vulnerability will be graded on the following 5-tier scale: critical, high, moderate, low and non-qualifying. The detailed criteria for assessment are listed below.

Critical

Rating: 9-10, SecCoin: 1080~1200

Extra cash reward (Currency: CNY)

1) 30,000 CNY - 100,000 CNY: Critical vulnerabilities in key Tencent mobile applications (Mobile QQ for Android / iOS, Wechat and QQ Browser for Android / iOS)
2) 10,000 CNY - 30,000 CNY: Critical vulnerabilities in Tencent web applications and key desktop applications (Tencent QQ standard version for desktop user)

This category includes:

1) Vulnerabilities that permit directly taking over Tencent servers or give access to client via exploiting Tencent applications.

Examples: Remote code execution, webshell uploading and execution, exploitable remote buffer overflow, exploitable ActiveX control stack overflow, exploitable Use after Free in browser, remote kernel exploits and other types of remote code execution caused by logic flaws.

2) Vulnerabilities that result in leakage of highly sensitive data.

   Examples: SQL injections which allow an attacker to gain unrestricted access to highly sensitive data stored in crucial databases.

3) Logic flaws with serious impact.

   Examples: Vulnerabilities that permit sending messages to other users via spoofed QQ / Wechat ID, vulnerabilities that permit sending arbitrary tips / feeds to other users via spoofed QQ / Wechat ID, vulnerabilities that permit resetting passwords of other user’s QQ / Wechat account.

High

Rating: 6~8, SecCoin: 360~480

Extra cash reward (Currency: CNY)

1) 10,000 CNY - 30,000 CNY: High-quality vulnerabilities in key Tencent mobile applications (Mobile QQ for Android / iOS, Wechat and QQ Browser for Android / iOS)

This category includes:

1) Vulnerabilities directly giving access to credentials of other users.

   Examples: Stored XSS in key business or web applications (e.g. Wechat, QQ Mail, Qzone and main website of Tenpay), SQL injection in normal Tencent web applications.

2) Unauthorized access to sensitive information.

   Examples: Vulnerabilities allowing unauthorized access to service management panel at the back-end.

3) High-impact vulnerabilities that leak sensitive information

   Example: Exploitable sensitive data leaking.

4) Local code execution.

   Examples: Exploitable stack overflow, use after free, double free, format string, local privilege escalation, DLL hijacking related to file association (Scenarios, ranging from loading non-existed DLL files to loading DLL without verification, are excluded) and other types of local code execution caused by logic flaws.

5) Vulnerabilities that permit gaining privilege of the client directly.

   Examples: Remote code execution, remote buffer overflow, exploitable ActiveX control stack overflow, exploitable Use after Free in browser, remote kernel exploits and other types of remote code execution caused by logic flaws.

6) Cross-site scripting in key mobile / desktop applications that permit obtaining sensitive data or performing sensitive operations (Definition of key mobile / desktop applications please refer to the following part).

Moderate

Rating: 3~5, SecCoin: 45~75

This category includes:

1) Vulnerabilities requiring user interactions that permit obtaining users' credentials.

   Examples: Reflected cross-site scripting (reflected DOM-based XSS), JSON Hijacking, CSRF that could perform sensitive operations, stored cross-site scripting in normal applications.

2) Remote denial of service in applications, leakage of sensitive information,

   Examples: Remote denial of service in kernel, cross-site scripting in applications that permit obtaining sensitive information or performing sensitive operations.

3) Leakage of moderate-impact information.

   Examples: Password stored as plaintext on the client, password transmitted in plaintext, leakage of compressed files which contain sensitive source codes.

Low

Rating: 3~5, SecCoin: 45~75

This category includes:

1) Vulnerabilities only being effective in specific browsers (e.g. IE6) that permit obtaining credentials of users.

Examples: Reflected XSS (including reflected DOM-XSS), stored XSS in normal Tencent applications.

2) Leakage of small amount of low-impact information.

   Examples: Full path disclosure, leakage of SVN files, disclosure of phpinfo or logcat information.

3) Local denial of service in Tencent PC or mobile applications.

   Examples: Local denial of service caused by miss-configured component permissions.

4) Unauthorized access.

   Examples: Bypassing proactive protection in applications, open redirectors, open redirectors via bypassing malicious websites blacklist (Ps. If it can only be used to redirect to a normal website, the open redirectors are invalid. It can be tested with the Proof of Concept:

   http://www.qq.com_521_qq_diao_yu_wangzhan_789.com.

   If the web page could be redirected to the website above, the service can be considered vulnerable).

5) Bugs that contain potential risks but are hard to exploit.

   Examples: Self-XSS that are both exploitable and can be easily spread, CSRF that can hardly perform sensitive operations, remote code execution requiring MITM with valid Proof of Concept submitted.

Non-qualifying

Rating: 0

This category includes:

1) Bugs that do not have security impacts.

   Examples: Bugs regarding the encoding of the page, failure in opening the web page, failure in specific functions.

2) Vulnerabilities that cannot be exploited.

   Examples: Scanning system reports that are without practical meanings (e.g. the version of Web Server is out-of-date), Self-XSS, JSON Hijacking that cannot give access to sensitive information, CSRF that cannot perform sensitive operations (e.g., favoriting, adding the item to the cart, subscribing unimportant businesses or services, modifying profile of the user of unimportant business), leakage of source code that can hardly be exploited, leakage of IP / domain of intranet, phishing via HTTP Basic Authentication dialogue, issues related to trust of the path of the applications, leakage of logcat information without sensitive information.

3) Wild guess without any proofs.

   Example: Inferred vulnerabilities based on the fact that QQ account getting hacked.

4) Applications that are not belong to Tencent.

Assessment standard for Discuz!

Under the background that Discuz!, developed by Comsenz Inc., is widely applied in Tencent online businesses and services, the impact will be comparatively high, if there is vulnerability. As a result, TSRC launched the special assessment standard for Discuz!. However, vulnerabilities in non-Tencent sites powered by Discuz! or unofficial plugins are not eligible in this standard.

Eligible versions included in this standard are listed in the table below. The symbol "√" means that fix for the security bugs will be shipped after they are confirmed. Nevertheless, the "×" means that there won' t be any patches. "Normal issues" cover vulnerabilities which are ranked as "Moderate" or "High" by TSRC, whereas "Critical issues" are these vulnerabilities ranked as "Critical" . The range includes:

Discuz! Version	.Maintenance Level	
	Normal issues	Critical issues
Discuz! X3.2	√	√
Discuz! X3.1	√	√
Discuz! X3.0	√	√
Discuz! X2.5	×	√
Discuz! X2	×	√
Discuz! X1.5.1	×	√
Discuz! X1.5	×	√

Assessment standard is listed as follows:

Severity	Impacts	Example	Rating
Critical	Taking over the server	Direct / limited arbitrary code execution, direct / limited arbitrary command execution	20 ~ 30
	Obtaining data in databases	SQL injection	20 ~ 25
High	Providing direct access to the information of manager and users	Stored XSS	10 ~ 15
	Unauthorized access	Sensitive operations that are performed in the role of manager.	10 ~ 15
Moderate	Obtaining credentials with user interaction	Reflected XSS	6 ~ 10
	Forgery of users' credentials	CSRF with substantial risks	6 ~ 10
	Leakage of	Normal leakage of information	3~6

	information		

Assessment standard for vulnerabilities of general software

1) Generally, the bug bounty program for vulnerabilities of general software covers all common software. Nevertheless, when investigating and rewarding, priority will be given to the software listed as follows:

   a) Operation systems: Linux, iOS, Android

   b) Web server: Apache, Nginx, Tomcat

   c) Storage system: MySQL, Memcached

   d) Coding language: PHP, Java

   e) Clouds and virtualization software: Xen, Hadoop

   f) Other critical software: OpenSSL, Struts

2) Reports, rated as “Critical” or “High” (the vulnerabilities that can be exploited remotely and have high-impact), should be submitted via TSRC if the submitter wants to be rewarded. More details please refer to the *assessment standard for Tencent applications* mentioned above.

3) Vulnerabilities that haven’ t been disclosed or reported to other organizations or institutions. In addition, valid Proof of Concept should be submitted.

4) Extra cash reward will be granted to the reporter of vulnerabilities of general software with huge impact. Additionally, the maximum amount of bounty is 500,000 CNY. Meanwhile, to assist these projects in improving their security, in the name of the reporter, TSRC will donate an equal number of bounty to the

affected vendors. (If the affected software are commercial products or the vendor decline the donation, TSRC will donate the same amount of funds to other charity projects).

Assessment standard for security intelligence

Security intelligence, including, but not limited to, useful information about vulnerabilities, attacks, identity of attackers, methods of attacks, technology of attacks, refers to the intelligence related to Tencent applications and services mentioned here. According to the severity and information provided, detailed criteria are listed as follows:

Severity	Coverage of the information	Example	Rating
Critical	Information about the incident of the servers, coupled with the details about related methods of attack.	Providing information about the servers being compromised. In addition, features of behavior, which contribute to a quicker investigation of the issue, are provided.	9~10

	Information about the leakage of data stored in important databases, coupled with related details, including names or files of the databases.	Providing the information about the fact that the databases are compromised. In addition, details about the databases, which contribute to a quicker investigation of the issue, are provided.	
	Information about critical logic flaws in financial applications.	Critical vulnerabilities in Tencent payment applications.	
High	Worm spreading, coupled with information about the links of the worm etc.	The outbreak of Internet worm incident caused by stored XSS in key applications or services.	6~8
	Information about the massive leakage of users' credentials, together with information about the exploiting code.	The massive leakage of credentials caused by vulnerabilities.	

Moderate	Novel attack methods or techniques which could contribute to the optimization of protection system or defense of critical/high-impact risks	Novel attack methods, which include information about new types of Webshell, DDoS etc.	3~5
Low	Information about the attackers	The QQ and telephone number of the attackers.	1~2

General Principles of Grading Standards

1) The Grading Standards are only specific to threat intelligence that affects Tencent products and businesses. Domain names include but not limited to *.qq.com, *.tencent.com, and *.tenpay.com. The servers include servers operated by Tencent. The products include client products directly released by Tencent. The threat intelligence which does not affect Tencent products and businesses will not be included.

2) The important client products refer to QQ, Mobile QQ, WeChat and Mobile QQ Browser. In addition, non-updated client products (including but not limited to QQ Images, QQ of Android HD version, Enterprise Email of iOS version, Friends Network of android version, QQ BianMin, Mobile QQ Browser of international edition, QQ Cyclone, etc.) will not be included, and their security vulnerabilities will not be fixed, in principle.

3) The products and services which do not directly released by Tencent, or developed by the third-party on Tencent platform (the domain name is generally *.Qzoneapp.com), are not included.

4) Common vulnerabilities (such as vulnerabilities of discus, and vulnerabilities generated by the same source) are generally counted as ONE vulnerability.

5) In the case that more than one person reports the same client product vulnerabilities (including PC and mobile) caused by third-party libraries (such as libpnp, zlib, libjpeg, and so on), which can be fixed by upgrading or replacing, the reward will be given to the first person who accomplish a qualified reporting. And all the vulnerabilities of same type will be counted as ONE vulnerability, whose severity rating will be assessed based on the maximum severity rating.

6) In the case that more than one person reports the same common vulnerabilities caused by mobile end system, such as UXSS of webkit and code execution, the reward will be given to the first person who accomplish a qualified reporting. The same vulnerability reports of other products will not be scored.

7) Since the assessment of client product vulnerability is more complex and involves many other departments, please understand that the time needed to assess may be longer than that of web vulnerability and sometimes TSRC may not come to a conclusion as scheduled. Therefore, a qualified report including poc/exploit and detailed analysis will be appreciated and help speed processing time. In contrast, a report which is lack of poc/exploit and detailed analysis will get a lower score.

8) If you submit more than one vulnerability of the same client product over the same period, please enclose the key code information that triggers the

vulnerabilities along with the report, which will help clarify whether they are the same vulnerabilities and speed processing time.

9) The security issues caused by third-party common vulnerabilities, are scored based on the reward standards of common vulnerability.

10) If the reporter review and find out that the security issue (The Status: fixed) is still found or not fixed, the issue he/she submits will be scored as a new security vulnerability.

11) In the case that more than one person reports the same security vulnerability, the reward will be only given to the first reporter. And security vulnerabilities that have been revealed to the public are not scored.

12) The scanning reports without any proof of actual harm will be ignored.

13) The following activities on the pretext of security testing are not allowed, against which Tencent will reserve the right to take further legal action.

    -To damage the interests of users by using security vulnerabilities.

    -To affect the normal operation of Tencent business.

    -To disclose the security issues before they are fixed.

    -To use security vulnerabilities to steal user data and other activities.

Dispute Resolution Policy

During the processing of threat intelligence, if the reporter has any objection to process, assessment, grading, etc., please feel free to contact TSRC by the comment function or "One-Click Contact US" button on the report page. TSRC will deal with it with the principle of **the priority interests of the reporters**. And a common ruling from the third party may get involved when necessary.

FAQ

Q: Will the information of threat intelligence be made public?

A: In order to protect users’ interests, the information of threat intelligence will not be disclosed until the security issues are fixed. Once they are fixed, the reporters can make it public. And TSRC recommends the reporters make them public in the form of academic technical articles.

Q: What is the relationship between TSRC and other security teams?

A: Tencent security is inseparable from the support and help from the entire industry. TSRC hopes to deepen cooperation with various security groups to jointly promote the development of the security industry. At present TSRC has cooperated with some security groups and will have more cooperation in the future.