2022

RFC 2350 CSIRT Blibli.com

VERSION 2.0

SEPTEMBER 2022

CLASSIFICATION: PUBLIC

CSIRT BLIBLI.COM, CSIRT FOR THE PT GLOBAL DIGITAL NIAGA

1. Document Information

This document contains a description of CSIRT Blibli.com in accordance with RFC 2350. It provides basic information about CSIRT Blibli.com, the roles and responsibilities, and the channels of communication.

1.1. Date of last update

This document is version 2, which is an update from the previous document published (v.1.0) in 7th May 2021. Document v.2.0 published in 30 September 2022.

1.2. Distribution of List Notification

N/A

1.3. Locations where this document may be found

The current version of this document can be found at:

https://github.com/bliblidotcom/CSIRT-RFC2350/blob/main/Blibli-RFC2350.txt

1.4. Document Authenticity

There are 3 types of original documents: in Indonesian, in English, and in Indonesian as txt files. the three documents. The three of documents have been signed with CSIRT Blibli.com's PGP Key. For more details, please see in Section 2.8

1.5. Document identification

This document contains some attributes, following detail:

Title	:	RFC2350 CSIRT Blibli.com
Version	:	2.0
Document Date	:	30 September 2022
Expiration	:	This document is valid until superseded by a later version

2. Contact Information

2.1. Name of the Team

Full Name	:	Cyber Security Incident Response Team - Blibli.com
Short Name	:	CSIRT Blibli.com

2.2. Address

Gedung Sarana Jaya Lt. 2 Jl Budi Kemuliaan 1 No. 1, Gambir, Jakarta Pusat, DKI Jakarta, Indonesia, 10110

2.3. Timezone

Jakarta, Indonesia (GMT+7)

2.4. Phone Number

+62-21-50881370

2.5. Facsimile Number

N/A

2.6. Other Telecommunication

N/A

2.7. Email Address

csirt@gdn-commerce.com

2.8. Public keys and encryption information

We use PGP for functional exchanges (notifications, incident reporting, etc.) with our peers, partners and constituents.

Bits	: ECC with ed25519 curve
Key ID	: 6C1B FF5F 9288 EF68
Key Fingerprint	: 521D 5789 07E8 29FF 58EF 9E69 6C1B FF5F 9288 EF68

Blok PGP Public Key :

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEYLh8hBYJKwYBBAHaRw8BAQdAWWuz90wSsQ4U0tVWudzo8ncBbIXyTiTwPtK0

T58gbia0W0NTSVJUIEJsaWJsaS5jb20gKEN5YmVyc2VjdXJpdHkgSW5jaWRlbnQg

UmVzcG9uc2UgVGVhbSBCbGlibGkuY29tKSA8Y3NpcnRAZ2RuLWNvbW1lcmNlLmNv

bT6IlAQTFgoAPBYhBFIdV4kH6Cn/WO+eaWwb/1+SiO9oBQJguHyEAhsDBQsJCAcC

AyICAQYVCgkICwIEFgIDAQIeBwIXgAAKCRBsG/9fkojvaB1+APwLQlLbUz6Dxc7x

p1QFUZKdJAl7VkrtF9PvEF6thA2lcwEAomyXpd6OrP/wyDc3O6E5JYX8TfyedMXD

+npdLtZrYwK4OARguHyEEgorBgEEAZdVAQUBAQdA4K/iBUjmPc3Tp0YV78OuLkPA

2NsSG9Zzf+nIxI7x2iQDAQgHiHgEGBYKACAWIQRSHVeJB+gp/1jvnmlsG/9fkojv

aAUCYLh8hAIbDAAKCRBsG/9fkojvaB23AP4nc1AaBwwIRvfCxXYGSM2fVRlFR2tX

clsRYkEotFHxkgEApQoXBRo2wolOh0P+EYPVF3Dn9sHbYZ26+3x3s3CBXwk=

=vhQT

-----END PGP PUBLIC KEY BLOCK-----
```

PGP key file is available on :

https://github.com/bliblidotcom/CSIRT-RFC2350/blob/main/CSIRT-Blibli.pub

2.9. Team Members

The Head of CSIRT Blibli.com is Rendra Perdana Satria, who assisted by a CSIRT team of 40 staff members.

2.10. Other Information

N/A

2.11. Contact Recommendation

We recommend method to contact CSIRT Blibli.com by email on csirt@gdn-commerce.com or by phone on +62-21-50881370 that standby on 24 hours.

3. Charter

3.1. Mission Statement

3.1.1. Vision

Improve the e-commerce experience through enhanced the information and cybersecurity.

3.1.2. Mission

Blibli.com's CSIRT missions are:

1. Provide technology services that aim to build cyber resilience and reliability that support business goals.
2. Provide cyber education and awareness to employees and other related parties with the aim of increasing cyber resilience.
3. Provide information on finding vulnerabilities, potential attacks and information on other cyber intelligence aimed at creating a cyber resilience ecosystem.

3.2. Constituency

Blibli.com CSIRT constituents include:

1) PT Global Digital Niaga
2) PT Global Kassa Sejahtera
3) PT Digital Otomotif Indonesia

3.3. Sponsorship and/or affiliation

Blibli.com's CSIRT funding by privately sourced

3.4. Authority

a) Determine the level of information security assessment on current or future business processes
b) Conduct a security level assessment of the information system that is made in-house, or rented/purchased by a third party
c) Supervise and actively intervene the information system operations in order to fulfill cyber resilience and reliability that supports business goals
d) Plan, create, and operate the design of cyber defense mechanisms (cyber defense-in-depth)
e) Implement cyber security awareness programs with relevant stakeholders
f) Have full authority to carry out internal and external coordination and intervention, access to data and systems in terms of handling cyber incidents

4. Policy

4.1. Types of incidents and level of support

Blibli.com CSIRT serves the following types of cyber incident handling:

- □ Main Services
    - X Cybersecurity Alert
    - X Cybersecurity Incident Handling
- □ Additional Services
    - X Handling of electronic system vulnerabilities
    - X Handling digital artifacts
    - X Notification of potential threats observation
    - X Attack detection
    - X Cybersecurity risk analysis
    - X Consultation on cyber incident preparedness
    - X Building cyber security awareness

4.2. Co-operation, interaction and disclosure of information

CSIRT Blibli.com will be cooperate and share information with CSIRT or other organizations in the scope of cyber security. All information received by CSIRT Blibli.com will be kept confidential.

4.3. Communication and authentication

For ordinary communication to CSIRT Blibli.com can use e-mail without special data encryption (conventional e-mail) and telephone. However, communications containing sensitive/restricted/confidential information may use PGP/RSA encryption on e-mails or e-mail attachments.

5. Services

5.1. Main Services

The main services of CSIRT Blibli.com are:

5.1.1. Cybersecurity Alert

This service will be implemented by Blibli.com CSIRT in the form of a warning of a cyber threat to the owner/operator of the electronic system.

5.1.2. Cybersecurity Incident Handling

Cyber incident handling services cover the full cycle of incident handling. Handling can be carried out on-site directly or providing suggestions for handling for follow-up.

5.2. Additional Services

The additional services of CSIRT Blibli.com are:

5.2.1. Handling of electronic system vulnerabilities

This service covers coordination, analysis and technical recommendations in order to strengthen aspects of security control (security control) both in technical and non-technical (Policy/Governance) scope.

In general, this treatment is divided into:

1) Temporary vulnerability reporting by constituents' electronic system owners/operators
2) Vulnerability handling services as a follow-up to audit activities or vulnerability assessments

5.2.2. Handling digital artifacts

Digital artifact handling services are carried out in order to maintain as well as possible the chain-of-custody process that may be needed in the context of investigations by law enforcement or as a means of technical investigation of incidents.

5.2.3. Notification of potential threats observation

This service is provided an observations based on the cyber intelligence function of CSIRT Blibli.com on digital assets belonging to constituents.

5.2.4. Attack detection

This service is provided with the aim of being a function of estimating the constituents' attack surface, this service is provided periodically in accordance with the compliance audit period

5.2.5. Cybersecurity risk analysis

This service is provided with the aim of being a function of estimating the constituents' attack surface, this service is provided periodically in accordance with the compliance audit period

5.2.6. Consultation on cyber incident preparedness

This consulting service is provided in order to help constituents to have sufficient preparedness in dealing with cyber incidents

5.2.7. Building awareness and concern for cyber security

This service is provided to constituents in order to build people-process-technology to support sustainable information security awareness education programs

6. Incident Reporting

Cybersecurity incident reports can be sent to csirt@gdn-commerce.com by attaching at least:

a) Detail information: Full Name, Position, Phone Number and origin Constituents
b) Incident evidence such as photos or screenshots or log files found
c) Evidence or other information in accordance with incident handling needs or applicable regulations

7. Disclaimer

a) CSIRT blibli.com carries out incident response activities by applying the principle of confidentiality as a working principle, information sharing with parties will be carried out by applying the principle of need-to-know

b) CSIRT blibli.com provides consulting services with a limited scope with the aim of cyber resilience with the maximum effort, we cannot guarantee the exact end result of the work listed on the service list

c) We are not responsible for the veracity and/or speed of the reports regarding the dissemination of threat information

d) CSIRT blibli.com only provides communication facilities through the channels listed in RFC2350, we are not responsible for communications on behalf of CSIRT Blibli.com through other channels

rendra.satria@gdn-commerce.com
2022.10.06
10:44:07 +07'00'