CYBERSECURITY
PHILIPPINES CERT®

CSP-CERT RFC 2350 PROFILE

TLP: WHITE
Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

TLP: WHITE information may be distributed without restriction, subject to copyright controls.

Table of Contents

1. Document Information

This document contains a description of CSP-CERT in compliance with RFC 2350[1]. It provides basic information about CSP-CERT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1. Date of Last Update

Version 1, published on Wednesday, March 28, 2018.

1.2. Distribution List for Notifications

Please send any questions about updates to the CSP-CERT e-mail address:
contact_us@cspcert.ph

1.3. Locations where this Document May Be Found

The current version of this document is always available at:
https://www.cspcert.ph/rfc2350/CSP-CERT-RFC2350.pdf

1.4. Authenticating this Document

A PDF version of this document has been signed with the GPG key of contact_us@cspcert.ph and can be found at:
https://www.cspcert.ph/rfc2350/CSP-CERT-RFC2350.pdf

The signature is available at:
https://www.cspcert.ph/rfc2350/CSP-CERT-RFC2350.pdf.sig

[1] https://www.ietf.org/rfc/rfc2350.txt

2. Contact Information

2.1. Name of the Team

Cyber Security Philippines - Computer Emergency Response Team

2.2. Address

Level 10-1 Fort Legend Tower
31st Street & 3rd Avenue, Bonifacio Global City,
Taguig City, 1634 Philippines

2.3. Time Zone

(UTC +08:00) Manila, Philippines

2.4. Telephone Number

CSP-CERT Hotline Number: (+632) 224-5637

2.5. Facsimile Number

(+632) 224-5638

2.6. Other Telecommunication

Facebook:
https://www.facebook.com/cspcert

LinkedIn:
https://ph.linkedin.com/company/cybersecurityphilippines-cert

2.7. Electronic Mail Address

Please send non-incident related email to:
contact_us@cspcert.ph

Please send incident reports to:
emergency@cspcert.ph

2.8. Public Keys and Encryption Information

Please encrypt any sensitive email/s with CSP-CERT's PGP key and send to contact_us@cspcert.ph or emergency@cspcert.ph

CSP-CERT's Public Key is available at Section 4.3 of this document.

Please sign messages using the respective keys for contact_us@cspcert.ph or emergency@cspcert.ph provided in this document.

2.9. Team Members

No public information is provided about CSP-CERT team members.

2.10. Other Information

Further information about CSP-CERT can be found at: https://www.cspcert.ph/

2.11. Points of Customer Contact

The preferred method for contacting CSP-CERT is through email. The use of GPG/PGP encryption when communicating with CSP-CERT is highly encouraged.

For memberships, partnerships, grants and other related sponsorships or general inquiries, please get in touch with our Program Development group at contact_us@cspcert.ph

For Breaches or any urgent Cyber Crime activity please contact our CERT® Response Center at emergency@cspcert.ph

CSP-CERT hours of operation are generally restricted to regular business hours: 09:00 to 17:00 Monday to Friday except public holidays.

3. Charter

3.1. Mission Statement

The primary purpose of CSP-CERT is to Secure the Filipino Nation by means of studying and solving problems with widespread cybersecurity implications, research and provide advisories on security compromises under the Philippine ASN.

CSP-CERT also collaborates closely with various local government units, law enforcement, schools and universities to help improve the cybersecurity advocacy in the Philippines with the aim of developing skills for cyber defense and future employment of Filipinos.

3.2. Constituency

CSP-CERT constituency is all internet users in the Philippines which includes all sectors and home users.

3.3. Sponsorship and/or Affiliation

CSP-CERT is a non-profit CSIRT recognized as the first registered CERT in the Philippines under the Division of the Software Engineering Institute (SEI) located in Carnegie Mellon University

CSP-CERT is currently affiliated with Global and ASEAN CERT, Honeynet Project and pending applications for Asia Pacific CERT and First.Org

4. Policies

4.1. Types of Incidents and Level of Support

The level of support provided by CSP-CERT will vary depending on the type and severity of the security incident or issue, its potential or assessed impact and the resources available to CSP-CERT at the time.

4.2. Co-operation, Interaction and Disclosure of Information

Regardless of priority, all incoming information is handled as CONFIDENTIAL by CSP-CERT.

When reporting an incident of sensitive nature, please state explicitly (for example, using the label CONFIDENTIAL or SENSITIVE in the subject field of the email) and if possible, use encryption as well.

4.3. Communication and Authentication

For secure communications, provided below is CSP-CERT's PGP keys.

The public key of contact_us@cspcert.ph is available at:
https://www.cspcert.ph/rfc2350/cspcert-contact_us-public.asc

The public key of emergency@cspcert.ph is available at:
https://www.cspcert.ph/rfc2350/cspcert-emergency-public.asc

5. Services

5.1. Digital Forensics and Incident Response

CSP-CERT assists organizations in handling and responding to breaches and act as subject matter expert to detect, respond and secure networks from various compromises.

5.2. Proactive Activities

Conducting Speaking Engagements and Events, Malware Research, providing advisories and articles for the constituency.

List of speaking engagements and talks provided by CSP-CERT members and volunteers is available at:
https://www.cspcert.ph/events.html

The list of Malware Research conducted by CSP-CERT members and volunteers is available at:
https://www.cspcert.ph/malware-research.html

The list of advisories is available at:
https://www.cspcert.ph/advisories.html

The list of articles is available at:
https://www.cspcert.ph/articles.html

6. Incident Reporting Forms

Not Available.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CSP-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information it provides.