WIN CSIRT RFC-2350

1. About this document

1.1 Last updated: This is version 2.0 of 09/22/2023

1.2 Distribution list for notifications: The changes to this document are not distributed via an email list. Any specific questions or comments, please contact csirt@winempresas.pe (This mailing list is moderate).

1.3 Document location: The latest version of the document is published at:

English: https://winempresas.pe/files/csirt/rfc/english/WIN-CSIRTdescription.pdf

Spanish: https://winempresas.pe/files/csirt/rfc/spanish/WIN-CSIRTdescription.pdf

2. Contact information

2.1 Team name: "**WIN CSIRT",** WIN EMPRESAS computer security incident response team.

2.2 Address: Main office, Av. Jose Gálvez Barrenechea 645 - San Isidro - Lima - Peru

2.3 Time zone: UTC -5. Lima/Peru.

2.4 E-mail: Information and incidents: csirt@winempresas.pe

Fingerprint	A835862C72AF839966F6DCFF6266A87D7BD98FFB
KEY ID	6266 A87D 7BD9 8FFB

2.5 Telephone: +51 01 680-9866

2.6 Team members: A complete list of team members is not publicly available. Team members will identify themselves to the reporting party with their full name in an official communication about an incident.

2.7 Customer contact points:

- Email -> Preferred method
- Phone -> Secondary method

If urgent assistance is required, put "**urgent**" in the subject line. If it is not possible (or not advisable for security reasons) to use email, you can contact WIN CSIRT by telephone during the established business hours. Phone messages are checked more frequently than email.

The operating hours of the WIN CSIRT are generally limited to normal office hours (09:00-18:00 Monday through Friday, except holidays). However, in case of critical incident or contractual service, the operation is 24*7*365.
If possible, when submitting your report, use the form mentioned in section 6.

3. Charter

3.1 Mission statement:

WIN CSIRT's mission is to actively support the cyber-resilience activities of our internal and external customers. To achieve this, we have the following objectives:

- Help our customers strengthen their early detection capabilities to reduce cybersecurity risks by implementing proactive controls and measures.
- Help WIN EMPRESAS's customer community respond to these incidents when they occur.
- Support our customers' operations recovery activities so they can achieve their business objectives in information security and business continuity.

3.2 Constituency:

The jurisdiction of WIN CSIRT are: internal and external clients, from the public or private sector. However, it should be noted that, despite the above, WIN CSIRT services will primarily be provided for WIN EMPRESA's data center systems and other data center or computer center locations of customers who are subscribed to the CSIRT services we provide. In the area of metropolitan Lima and Callao. For other locations further away and/or in the context of a pandemic or similar; We can act, as long as we are provided with secure remote access to the infrastructure where the incident has occurred.

3.3 Sponsoring Organization: WIN CSIRT is sponsored by WIN EMPRESAS.

3.4 Authority: WIN CSIRT operates under the auspices of and with authority delegated by WIN EMPRESAS. WIN CSIRT looks forward to working in cooperation with WIN EMPRESAS system administrators and users and with the corresponding client teams and, to the extent possible, avoiding authoritarian relationships. However, if circumstances warrant, WIN CSIRT will appeal to WIN EMPERESAS to exercise its authority, direct or indirect, as necessary.

All members of WIN CSIRT belong to the cybersecurity and communications team of the Cloud business unit of WIN EMPRESAS and have all the powers and responsibilities assigned according to the systems they manage or failing, are members of the management of WIN EMPRESAS.
Community members who wish to appeal to WIN CSIRT actions should contact the head of cybersecurity and communications services. If this resource is not satisfactory, the matter may be referred to the Cloud and Services operations manager.

4. Policies

4.1 Types of Incidents and Level of Support

WIN CSIRT is responsible for addressing various types of incidents and evaluates them according to criteria of dangerousness or criticality that are discussed with clients. The level of assistance provided will depend on both factors and the severity as determined by WIN CSIRT staff.
Resources, which influence the level of WIN CSRIT support, will be allocated according to the following priorities listed in decreasing order:

- Threats to the physical security of individuals.
- Massive or system-level attacks on any Management Information System, or any part of the backbone infrastructure.
- Massive or system attacks on any large public service machine, either multi-user or for exclusive use.
- Compromise of restricted confidential service accounts or software installations, particularly those used for WIN EMPRESAS applications containing confidential data, or those used for system administration.
- Denial of service attacks on any of the above three elements.
- Any of the above on other sites, originating in WIN EMPRESAS.
- Large-scale attacks of any kind, for example, ransomware, sniffing attacks, "social engineering" attacks, password cracking attacks.
- Threats, harassment and other crimes related to individual user accounts.
- Commitment of individual user accounts in multi-user systems and of desktop systems.
- Counterfeiting and misrepresentation, and other security-related violations of local regulations, for example, counterfeiting of websites, Netnews and e-mail, unauthorized use of bots.
- Denial of service on individual user accounts, e.g., mailbombing.

Incident types other than those mentioned above will be prioritized based on their apparent severity and extent.

4.2 Cooperation, interaction and disclosure of information:

WIN CSIRT will take appropriate measures to protect the information and identity of members of our community served. The information will be treated with absolute confidentiality in accordance with its classification. However, information will be freely shared when it will assist in resolving or preventing security incidents.

4.3 Communication and Authentication

The media available with WIN CSIRT are as follows:

- E-mail and phone described above.
- The authentication process is performed using PGP as the authentication mechanism.

5. Services

WIN CSIRT provides proactive and reactive services. Proactive services seek to anticipate any incident to prevent them, and reactive services are those that focus on monitoring, analyzing, categorizing, containing and responding to cyber threats. Below is a brief description of the services available:

5.1 Proactive Services:

5.1.1 Vulnerability Management

WIN CSIRT will analyze current and moving vulnerabilities to strengthen information security and reduce the risk of security breaches in partner organizations.

- Vulnerability discovery / research
- Vulnerability reporting
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

5.1.2 Knowledge Transfer

WIN CSRIT members will share and transmit information and experience through internal and external conferences.

- Awareness raising
- Training and education
- Exercises

5.2 Reactive Services:

5.2.1 Information security event management

WIN CSIRT will monitor and analyze security events occurring on a company's or collaborating entity's information systems and networks.

- Monitoring and detection
- Event analysis

5.2.2 Information security incident management

WIN CSIRT will identify, analyze, monitor, and respond to security incidents so that the integrity, availability, and integrity of an organization's data assets are not compromised.

- Receipt of information security incident report notification
- Analysis of artifacts and forensic evidence
- Mitigation and recovery
- Information security incident coordination
- Crisis management support

6. Incident Reporting Forms

To report and inform incidents, communication should be sent to: csirt@winempresas.pe

An internal Incident Reporting Form is also available called: Formulario de informe de seguridad WIN CSIRT.

7. Disclaimers

WIN CSIRT will take every precaution in the preparation of information, notifications and alerts. However, it assumes no liability for errors or omissions, or for damages resulting from the use of the information contained therein.