CERT.AZ description

as per RfC 2350

Contact

Cyber Security Service (CSS)

Computer Emergency Response Team (CERT)

Address

Block 702, Drogal lane

Baku, Azerbaijan

Telephone: +99412 4932056

+99412 4932057

Fax: +99412 4981800

E-mail: info@cert.az

www.cert.az

Published by

Cyber Security Service under Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan 2021

Contents

1. Document information

1.1. Date of Last Update

This is the 1.2 version, published March 3, 2021

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified

1.3. Location of the document

www.cert.az

2. Contact Information

2.1. Name of the Team

Short name: *CERT-AZ*
Full name: *Cyber Security Service*

2.2. Address

Azerbaijan, Baku, Drogal lane, block 702

2.3. Time Zone

UTC/GMT+04:00

2.4. Telephone Number

+99412 4932057
+99412 4932056

2.5. Facsimile Number

+99412 4981800

2.6. Other Telecommunication

Not applicable.

2.7. Electronic Mail Address

For Security incidents to: reports@cert.az
For Technical issues to: team@cert.az
For General inquiries and non-emergency issues to: info@cert.az

2.8. Public Keys and Encryption Information

The CERT-AZ has a PGP key.
User ID: team@cert.az
Key ID: 0xA5E67725
Fingerprint: 73B99C81E49F8EF3E3A761B9A4B1F6B0A5E67725

The key and its signatures can be found at public key servers like pgp.mit.edu.

2.9. Team Members

No information is provided about CERT.AZ team members in public.

2.10. Other Information

Further information about CERT.AZ can be found at: http://www.cert.az/en/about-us.html

2.11. Points of Customer Contact

An available way for contacting CERT.AZ is via e-mail.

reports@cert.az is available for security incident reports and related issue.
team@cert.az at is available for technical issues.
info@cert.az is available general inquiries and non-emergency issues.

If it is impossible (or advisable due to security reasons) to use e-mail, you can connect with us via telephone at 99412 4932057
99412 4932056

Hotline: 1654

Office hours for CERT.AZ are generally restricted to local regular business hours: Mon-Fri, 9 a.m. - 6 p.m.

3. Charter

3.1. Mission Statement

Service's mission is to create and defend a better and safer cyber environment in the country while:

- To coordinate the action of information infrastructure subjects,
- To report about existing and potential risks at country level,
- To educate public, private and other institutions in the field of cyber security and providing methodological assistance to them

3.2. Constituency

The constituency of CERT.AZ is basically public and private sector.
The main areas of responsibility of CERT-AZ are:

- Engages in reporting on existing and potential threats in the field of cyber security at country level, as well as educating the public, private and other institutions
- Collects and analyzes information incoming from users, software and hardware productions, similar structures in foreign countries and other sources, about cyber security attacks, illegal intrusions and malicious codes against Information systems and networks
- Analyzes widely used software and technical equipment and recommends how to avoid detected security vulnerabilities

3.3. Sponsorship and/or Affiliation

- CERT-AZ has been established under the Ministry of Transport, Communications and High Technologies (www.mincom.gov.az). It is funded on state budget.
- CERT-AZ is affiliated with FIRST, the global Forum of Incident Response and Security Team as a full member as well as TI (Trusted Introducer for European CERTs) as an accredited member and Anti-Phishing Working Group (APWG). CERT-AZ continues affiliations with various CSIRTs

around the world as needed. It also has cooperation with CERT Coordination Center.

3.4. Authority

CERT.AZ has a formal authority to advice:

- According to the Constitution of the Azerbaijani Republic
- The laws of the Azerbaijani Republic
- The decrees and instructions of the President of the Azerbaijani Republic
- The resolutions and instructions of the Cabinet of Ministers of the Azerbaijani Republic
- The international treaties which participant is the Azerbaijani Republic,
- The regulations on the Ministry of Transport, Communications and High Technologies of the Azerbaijani Republic the regulatory legal acts accepted by the Ministry, and this Provision.

4. Policies

4.1. Types of Incidents and Level of Support

We have an authority to solve all kind of security incidents which occur or threaten to occur. The level of support of CERT.AZ depends on the type and severity of the issue or incident, the type of constituent. Our organization is committed to keeping publicinformed of potential vulnerabilities.

4.2. Co-operation, Interaction and Disclosure of Information

In case of accomplishment of the tasks and implementation of the rights the Cyber Security Service interacts with the Ministry of Transport, Communications and High Technologies and the structures subordinated to it, central and local executive bodies, local government bodies and non-governmental organizations, the international organizations, and also the legal entities and physical persons specializing in information security field.

CERT.AZ makes relations with some other CSIRTs. We cooperate with Georgian, Iran, Israil and Bulgarian CERT's.

4.3. Communication and Authentication

For international communications ordinary precautions apply – like communicating to/via previously trusted and listed teams (TI) and using PGP. Key people know each other personally before any significant cooperation occurs.

5. Services

5.1. Incident Response

CERT-AZ defines, assesses and prioritizes all types of ICT incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1 Incident Triage

- Investigating whether incident is authentic
- Determining type of the incident
- Assessing the incident

5.1.2 Incident Coordination

- Determining and contacting involved organizations.
- Assisting contact with other organs including law enforcement, if needed.
- Make relations with media, if necessary.

5.1.3 Incident Resolution

- Following up the incident solution process.
- Collecting evidence and interpreting data
- Asking for reports

5.2 Proactive Activities

- to inform people about existing threats and incidents in the field of cybersecurity
- to publish alerts and incidents in our website related serious security threats
- to implement educational events about information security

For other information, follow http://www.cert.az/en/services.html

6. Incident Reporting Forms

For cybersecurity incidents: https://cert.az/report_cyber

For personal data breaches: https://cert.az/report_personalinfo

For reporting illegal content on the Internet: https://cert.az/report_spread

7. Disclaimers

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