CNCERT/CC 国家互联网应急中心

Partner

About Us

National Computer Network Emergency Response Technical Team/Coordination Center of China

1. Brief Introduction

The National Computer Network Emergency Response Technical Team/Coordination Center of China (known as CNCERT or CNCERT/CC) was founded in September 2002. It is a non-governmental non-profit cybersecurity technical center and the key coordination team for China's cybersecurity emergency response community. As a national CERT, CNCERT strives to improve nation's cybersecurity posture, and protect critical infrastructure cybersecurity. CNCERT leads efforts to prevent, detect, warn and coordinate the cybersecurity threats and incidents, according to the guideline of "proactive prevention, timely detection, prompt response and maximized recovery".

CNCERT has branches and offices in 31 provinces, autonomous regions and municipalities across mainland China. As the key coordination organization of China's cybersecurity emergency response system, CNCERT organizes enterprises, schools, non-governmental groups and research institutes that are specialized in cybersecurity and coordinates ISPs, domain name registrars and other emergency response organizations in a joint effort to build the cybersecurity emergency response system of China and handle major cyber security incidents.

As an important non-governmental organization to assist in the cross-border handling of cyber security incidents, CNCERT actively carries out international cooperation in cybersecurity and is committed to establishing a mechanism of prompt response and coordinated handling for cross-border cybersecurity incidents. CNCERT is a member of the world-renowned Forum of Incident Response and Security Teams (FIRST) and one of the founders of Asia Pacific Computer Emergency Response Team (APCERT). As of 2013, CNCERT has established "CNCERT International Cooperation Partnership" with 127 organizations in 59 nations and regions.

2. Mission Statement

Incident Detection: Leveraging on the cybersecurity detecting platform, CNCERT performs proactive detection of security incidents for critical infrastructure. It also discovers cybersecurity threats and incidents by sharing data and information with domestic and foreign partners and by receiving cyber security incident reports from domestic and foreign customers through hotline, fax, email and website.

Early Warning: By making comprehensive analysis of big data and acquiring information from multiple channels, CNCERT can warn cybersecurity threats, report cybersecurity incidents and analysis cybersecurity posture. It provides customers with such services as information on cybersecurity situation and sharing of cybersecurity technology and information.

Emergency Response: If incidents of serious threat are proactively discovered or received, CNCERT will respond in a timely manner and actively coordinate the handling. Priorities include incidents that affect Internet operation security, affect a large scope of Internet users, involve key government departments and critical infrastructure, cause major consequences users complaint, as well as all kinds of cybersecurity incidents reported by national emergency response organizations of foreign countries.

Security Evaluation: As a professional organization of cybersecurity evaluation, CNCERT provides security testing services for government departments, public institutions and enterprises guided by the principle of "supporting the regulatory, serving the society" and through scientific methods, standard procedures, impartial attitude, independent judgment and relative standards.

3. Incident Handling Procedures

Report: CNCERT has set up a 24*7 mechanism to accept the report of cybersecurity incidents. Both domestic and foreign users can report an incident to CNCERT in the following ways: website, email, hotline and fax.

Ø Website: http://www.cert.org.cn/

Ø Email: cncert@cert.org.cn

Ø Hotline: +8610 82990999, 82991000(EN)

Ø Fax: -8610 82990399

Acceptance: Cybersecurity incidents undertaken by CNCERT mainly include the following types: malware, defacement, backdoor, phishing, vulnerability, information destruction, denial of service attack, abnormal domain, router hijacking, unauthorized access, spam, mixed cyber security incidents and other cyber security incidents.

Handling: After confirming that the incident is true by sufficient evidences, CNCERT will perform emergency handling based on the prompt response mechanism which has established with domestic and foreign ISPs, domain name registrars and cybersecurity service vendors.

Feedback: When each of the three steps above - report, acceptance and handling - is completed, CNCERT will provide feedback to the reporter, including receipt of the report, whether it is accepted and for what reason, and the handling results.


Email: cncert@cert.org.cn Tel: +8610 82991000