CCN-CERT RFC 2350

1. Document Information

1.1. Date of last update: version 1.0, published 15th October 2019

1.2. Distribution Lists: There is no distribution channel to notify changes in this document. Changes are announced by means of notification in https//www.ccn-cert.cni.es

1.3. Location of the Document: The latest version of the document is published in:

- Spanish https://www.ccn-cert.cni.es/sobre-nosotros/rfc2350.html
- English https://www.ccn-cert.cni.es/en/about-us/rfc2350.html

1.4. Document Authentication: This document has been digitally signed by the CCN-CERT.

2. Contact Information

2.1. Team Name: CCN-CERT, Spanish Government CERT of the National Cryptologic Centre (CCN).

2.2. Address:

CCN-CERT, National Cryptologic Centre

National Intelligence Centre

C/Argentona, 30, 28023

Madrid

2.3. Time Zone: CET / CEST

2.4. Telephone Number: Not disclosed in public media.

2.5. Fax number: Not existing

2.6. Other Communications: Not existing

2.7. Email Addresses:

- Incident information exchange: incidentes@ccn-cert.cni.es
- General enquiries: info@ccn-cert.cni.es
- Other email addresses to contact the CCN-CERT: https://www.ccn-cert.cni.es/en/about-us/contact.html

2.8. Public keys and encrypted information: contact e-mails and associated PGP keys are published at:

https://www.ccn-cert.cni.es/sobre-nosotros/contacto.html

2.9. Team Members: Not available

2.10. More Information: General information on the services provided by the CCN-CERT and on the organization itself is published on the website:

https//www.ccn-cert.cni.es.

2.11. Opening hours: The incident response team is available at the following schedules:

- Consultations about services: office hours (8.00h-18.00h)
- Incidents classified as low, medium or high danger[1]: office hours (8.00h-18.00h)
- Incidents catalogued with very high or critical danger: 24x7x365.

2.12. Community Contact Points: Communication between the CCN-CERT Team and the organisms it supports is mainly through:

- Mailbox associated with the subject to consult: https://www.ccn-cert.cni.es/en/about-us/contact.html
- Telephones provided during the accession process or incident support.

3. Constitution

Mission: The CCN-CERT is the Information Security Incident Response Team of the National Cryptologic Center, CCN, accountable to the National Intelligence Centre, CNI. This service was created in 2006 as the Spanish Government CERT, and its functions are listed in Law 11/2002 of the CNI, RD 421/2004 regulating the CCN, RD 3/2010 regulating the National Security Scheme (ENS), modified by RD 951/2015, and Royal Decree 12/2018 on the security of networks and information systems.

Its mission is to contribute to the improvement of Spanish cybersecurity, being the national alert and response centre that cooperates and helps to provide quick and effective solutions to cyber attacks and counter cyber threats in a proactive manner. It provides state coordination between the different Incident Response Teams or existing Cybersecurity Operations Centres for incidents of special relevance.

All this, with the ultimate aim of guaranteeing a safer and more reliable cyberspace, by protecting classified information and sensitive information, preserving the Spanish heritage, training experts, implementing security policies and procedures, and employing and developing the most appropriate technologies for this purpose.

3.2. Community to which it provides services:

In accordance with the abovementioned regulations and Law 40/2015 on the Legal System for the Public Sector, to which Royal Decree 12/2018 refers, CCN-CERT is responsible for the

[1] Danger: as defined in CCN-STIC 817.

management of cyberincidents that affect the Public Sector systems or companies of strategic interest, as well as any other system in which classified information is processed.

In the case of essential services, the management of cyberincidents will be carried out by CCN-CERT in coordination with the National Centre for Critical Infrastructure Protection (CNPIC).

3.3. Sponsorship / Affiliation: The CCN-CERT is part of the National Cryptologic Centre (CCN), attached to the National Intelligence Centre (CNI).

Authority: The CCN-CERT authority derives from the following legislation:

- Royal Decree 3/2010, updated in R.D. 951/2015, regulating the National Security Scheme in the field of Electronic Administration (article 37).
- Royal Decree 12/2018, on the security of networks and information systems (Article 19. Obligation to notify)

4. Policy

4.1. Type of Incidents and level of support:

The type of cyberincidents on which the CCN-CERT acts are reflected in the guide CCN-STIC-817, in section 6.1 "Cyber-incident classification".

CCN-CERT, as a National Governmental CERT, partners with Spanish **public bodies and companies of strategic interest** to detect, report, evaluate, counter, handle and learn from information security incidents or cyber incidents that may affect their systems.

The level of support provided by the CCN-CERT and the response time will depend on the danger level of the incident and other factors set out in the Guide CCN-STIC-817 Cyberincident Management, according to the following criteria:

- Type of threat (malicious code, intrusions, fraud, etc.)
- Origin of the threat: internal or external.
- The security category of the systems affected.
- The profile of affected users, their position in the organizational structure of the entity and, consequently, their privileges of access to sensitive or confidential information.
- The number and type of systems affected.
- The impact that the incident might have on the organization, from the points of view of information protection, service protection, legal compliance and/or public image.
- The legal and regulatory requirements.

The CCN-CERT also provides information about the state of cybersecurity to your Community, in order to reduce technical (hardware and software), human and organizational vulnerabilities. To do this, it periodically notifies the following information:

- Warnings: Threats/vulnerabilities detected by the CCN-CERT itself or other CSIRTs.
- Alerts: the same as the previous epigraph, but with a higher criticality.
- Vulnerabilities: Daily from major manufacturers.
- Reports of malicious code.

- Good practice reports.
- Threat reports.

4.2. Cooperation, Interaction and Dissemination of Information: The information managed by the CCN-CERT is treated with absolute confidentiality in accordance with the policies and procedures for Incident Management established for the CCN-CERT, the policies and rules of the CCN and the security rules for the protection of classified information.

4.3. Communication and Authentication: The means available for communication with the CCN-CERT are:

- E-mail encrypted with the public keys dedicated to it and published on the web portal: https://www.ccn-cert.cni.es/en/about-us/contact.html
- Telephones provided during the accession process or incident support.

5. Services

5.1. **Prevention**

The CCN-CERT performes different activities in order to raise awareness and prevent any incident. Among them, the following stand out:

a) Security policy definition
b) Support and coordination for the treatment of vulnerabilities
c) Reports, alerts and warnings on new threats and vulnerabilities of information systems, compiled from various sources of recognized prestige, including their own.
d) Research and dissemination of best practices on information security.
e) Development of Security Guides with regulations, procedures and good practices.
f) Training and awareness-raising on cybersecurity for qualified professionals with different profiles and levels of training. It has basic training and two itineraries: management and specialization. This training is performed both in person and online and with specific streaming courses.
g) Organization and participation in cybersecurity conferences and congresses.
h) Web audits to the systems of the Public Sector.

5.2 Incident Management

The CCN-CERT provides technical and operational support in the different stages of the incident management process: detection, analysis, notification, containment, eradication and recovery. This process includes the evaluation of available information and its prioritization (triage), its validation and verification; the collection of the necessary additional evidence; communication with the relevant parties and, finally, the resolution of the incident.

It also advises the teams on the most appropriate actions; monitors the management of the incident and requests the relevant reports (the heads of the agency issue a Report of the

Cyberincident in which they must detail its root cause, its cost and the measures that the organization must take to prevent future cyberincidents of a similar nature).

5.3. Incident Coordination

The CCN-CERT coordinates incidents and also acts as the national coordinator of the different CERT and CSIRT capabilities or Security Operations Centres (SOC) in the public sector.

The CCN-CERT will act as the national coordinator of the technical response of the CSIRT in cases of special gravity concerning operators of essential services that require a higher level of coordination than the necessary in ordinary situations.

5.4. Monitoring

The CCN-CERT has developed an Early Warning System (EWS) for the detection of incidents in its community organizations. There are currently three aspects to the SAT:

- SAT-SARA. Monitoring of the Public Administration Intranet
- SAT-INET. Monitoring of the Internet outputs of the bodies attached to the service
- SAT-ICS. Monitoring of Industrial Control Systems.

5.5 Development of cybersecurity solutions and tools

The CCN-CERT coordinates and promotes the development of solutions which guarantee the security of systems and contribute to a better management of cybersecurity in any organization. These solutions are focused mainly on detection, analysis, auditing and information exchange.
A complete updated list of these tools can be found at:
https://www.ccn-cert.cni.es/en/tools.html

5.6 Forensic and malware analysis

The CCN-CERT has specialized equipment and experts to perform forensic analysis of equipment involved in complex incidents.
Likewise, the CCN-CERT has the ability to perform static and dynamic analysis of malicious code samples to generate detection patterns.

6. Incident reporting forms

Incident notification can be done via:

- Specific mailbox: incidentes@ccn-cert.cni.es
- LUCIA: Incident notification tool.
- Telephones provided during the adhesion process or incident support.

7. Disclaimer

The CCN-CERT Team is not responsible for any misuse of the information contained herein.

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2019.10.14 11:51:38 +02'00'