Nologin CSIRT - RFC 2350 - EN

December,2024

Index

1 Document Information

1.1 Object

This document describes the service provided by the Nologin Computer Security Incident Response Team in order to define its work and operations, organizational structure and contact forms. The format for this purpose complies with the RFC 2350 standard https://www.ietf.org/rfc/rfc2350.txt.

1.2 Update date

Updated on 7 november of 2024.

1.3 Distribution list

There is no distribution channel for notifying changes to this document. For any questions, please contact us through https://nologin.es/en/contact .

1.4 Document location

This document is available in https://www.nologin.es/en/cybersecurity-incident-management-csirt-as-a-service .

2 Contact Information

2.1 Identification data

- **Team Name**: Nologin-CSIRT
- **Address**: Avenida Ranillas, 1D, 3rd Floor, Av. Ranillas, 1D, office 3G, 50018 Zaragoza
- **Time Zone**: CET / CEST
- **Phone Number**: +34 976 51 24 33
- **Fax Number**: None
- **Other Communications**: None
- **Email Addresses**:
    - Incident management for the community: incident.csirt@nologin.es
    - Notice of information of interest to the CSIRT: communication.csirt@nologin.es
- **Public Keys and Information Encryption**: PGP keys availables in RedIRIS
    - incident.csirt@nologin.es: 093432C8A7858FFDF1A432977385A8FB0907BB78
    - communication.csirt@nologin.es: 76261009EAC4ACD43D28D273BEF5A84DB9D08E1E

2.1.1 Members

The CSIRT team at Nologin is made up of cybersecurity analysts grouped into different levels according to their functions and level of analysis. They are all managed by the CSIRT Service Manager and the Head of Cybersecurity at Nologin.

By this way, the service offered by Nologin-CSIRT has the next operational levels:

- Security Manager
- CSIRT Manager
- Information security experts (Level 3)
- Incident response specialists (Level 2)
- Cibersecurity analysts (Nivel 1)

2.1.2 Service hours

The CSIRT team at Nologin is available during the following hours:

- Cybersecurity service inquiries: Business hours (8:00 a.m. - 6:00 p.m.).
- Cybersecurity incidents: Extended hours (24x7x365).

2.1.3 Community Contact Points

The previously mentioned email addresses have been enabled for handling incidents and CSIRT inquiries.

3 Constitution

3.1 Misión

The Nologin CSIRT (hereinafter referred to as "Nologin-CSIRT") is a private incident response team that operates in both public organizations and private companies. Its establishment aligns with the mandate of Nologin S.L.U. to provide cybersecurity services aimed at managing the lifecycle of a cyber incident, thereby assisting clients in taking the correct and timely actions to minimize impact and prevent business and service losses.

Nologin offers both the expertise of its technical specialists and the leadership of its managers to properly handle a cybersecurity incident. Additionally, Nologin-CSIRT also provides cybersecurity services that assist in responding to incidents affecting the integrity, confidentiality, or accessibility of information.

Furthermore, Nologin-CSIRT offers proactive services that help companies manage cybersecurity prior to the detection of cyber incidents. These services include:

- Administration, operation, and enhancement of cybersecurity tools in accordance with the business and operational needs of the client.
- Automated responses based on SOAR tools to reduce response times and minimize impacts.
- Cyber intelligence communications to prevent and avoid imminent attacks.
- Advanced threat hunting and vulnerability lifecycle management.
- Security event monitoring and incident detection.
- Integration of products and services to enrich information.
- Compliance with standards and regulations.

3.2 Jurisdiction

The services provided by Nologin-CSIRT are aimed at entities, both public and private, that choose to engage in their hiring. The previously mentioned services will be tailored to the client after contracting to optimize results and ensure cybersecurity from a more "ad-hoc" perspective.

3.3 Authority

Nologin-CSIRT operates within Nologin S.L.U. and under the authority of the Security Manager and the company's Management.

4 Policies

4.1 Type of Incidents and Level of Support

The Nologin-CSIRT team continuously works on responding to any cyber incident that is reported, whether manually or automatically, through its services or affiliated entities. This response is carried out within the framework established by the CCN in the CCN-STIC-817 guide to ensure uniformity and proper handling.

According to a tiered escalation system, incidents are analyzed and prioritized based on the severity determined in the initial analysis, following the recommendations of CCN-CERT, the client's business, and the cybersecurity knowledge base maintained by Nologin-CSIRT.

Based on this initial categorization, the escalation and response time are determined. Companies and entities subscribed to Nologin's services will have prior agreements on the service level that ensure a response in accordance with the incident categorization, which will be determined, among other factors, by the type of attack, the impact, the severity, the credibility of the indicators, and the systems involved, among other parameters.

In this way, Nologin-CSIRT manages the entire lifecycle of the incident, from the initial handling to the final remediation actions.

4.2 Cooperation, Interaction, and Information Disclosure

The information handled by Nologin-CSIRT is confidential and private, and it is processed solely for the purpose of the contracted services, in accordance with Nologin's internal policies (supported by the Medium Level ENS certification and ISO 27001) and GDPR regulations.

During the execution of its mission, within RNS or First, Nologin-CSIRT may interact with other organizations, such as other CERT or CSIRT teams or intelligence services, to enhance its services and those of other entities, thereby improving the cybersecurity of all end clients.

In the Spanish national context, two reference CERTs have been established to which relevant information security and system incidents must be reported, with their competencies limited according to the type of organizations affected by the incidents. These organizations are:

- **INCIBE-CERT:** For citizens, organizations, and private sector companies.
- **CCN-CERT:** For public organizations and companies.

4.2.1 Information disclosure

Nologin S.L.U. understands and adheres to the Traffic Light Protocol (TLP) standard as a vital framework for sharing sensitive information responsibly. By employing TLP, Nologin ensures that

information is distributed with appropriate restrictions, fostering trust and safeguarding confidentiality. This approach enhances collaboration with CSIRTs (Computer Security Incident Response Teams) by enabling secure and efficient information exchange, supporting proactive responses to cyber threats while upholding industry best practices.

According whit it, these are TLP labels used in Nologin's communications:

a. **TLP:RED**: For the eyes and ears of *individual* recipients only, no further disclosure.

b. **TLP:AMBER**: Limited disclosure, recipients can only spread this on a need-to-know basis within their *organization* and its *clients*.

c. **TLP:GREEN** = Limited disclosure, recipients can spread this within their community.

d. **TLP:CLEAR** = Recipients can spread this to the *world*, there is no limit on disclosure.

4.3 Communication and Authentication

Nologin-CSIRT employs an internal information labeling system to appropriately and accurately distribute information through the various available channels. This ensures that the confidentiality and integrity of the information are not compromised in accordance with its internal policies, the General European Data Protection Regulation (GDPR), and the European NIS2 directive.

5 Provided services

There are two services provided by Nologin-CSIRT:

- Reactive activities
- Proactive activities

5.1 Reactive services

The reactive services provided by Nologin CSIRT guarantee a complete response to a cyber incident. To achieve this, Nologin-CSIRT coordinates the entire life cycle of the incident, as well as technically responding to the incidents needs.

Thus, Nologin monitors, detects, classifies, categorizes, analyzes, coordinates and responds to cyber incidents (monitoring and DFIR services). This complete management of the incident by Nologin guarantees correct coordination of containment and recovery, which minimizes the impact and secures the business.

5.2 Proactive services

Proactive services improve and secure resources in order to avoid and prevent possible future incidents.

5.2.1 Cyber Intelligence and Alerts

Nologin-CSIRT has internal deployed services that continuously analyze cyberspace in order to find any information that may affect the client's security. This service generates early alerts along with the necessary recommendations if, after an initial analysis, it is determined that any action is necessary.

5.2.2 Awareness

Compliance with internal policies, as well as cybersecurity awareness, are essential to eliminate security problems caused by bad practices in organizations.

Nologin-CSIRT also analyzes the business and structure of clients to offer appropriate awareness campaigns that minimize the risk of possible attacks.

5.2.3 Vulnerability Management and Audits

Nologin-CSIRT conducts a comprehensive review of the client's service to perform vulnerability discovery and audit tasks to address existing security issues before they are exploited by malicious actors.

In addition to providing the necessary categorization to prioritize all findings, Nologin-CSIRT provides recommendations for mitigation, and support during mitigation.

5.2.4 Cibersecurity development

Nologin-CSIRT is always developing new knowledge and skills to adapt the client's cybersecurity to new trends, in such a way that security is guaranteed at all times.

This objective is carried out by analyzing new threats together with the analysis of the client's service. The result is proactive improvements in tools (new monitoring, automation of responses, security architectures, etc.), as well as the design and implementation of new solutions that adapt to each scenario presented.

6 Incident Notification Methods

Incident notifications can be made through:

- **Specific Email Inbox:** incidents@ccn-cert.cni.es
- **ITSM** system enabled during the enrollment process
- **Phones:** Provided during the enrollment process or incident support.