1. DOCUMENT INFORMATION

1.1 DATE OF LAST UPDATE

This is version 1, 2022/04/20

1.2. DISTRIBUTION LIST FOR NOTIFICATIONS

Notifications of updates are submitted to the mailing list: cert@nexigroup.com

1.3. LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

The current version of this document is available internally within the constituency and its subsidiaries.

2. CONTACT INFORMATION

2.1. NAME OF THE TEAM

Full name: Nexi Payments CERT

Short name: Nexi Payments CERT

2.2. ADDRESS

Postal Address:

Nexi Payments S.p.A.

Via Gonin, 36

20147 Milano

Italy

2.3. TIME ZONE

Central European (GMT+0100 and GMT+0200 from the last Sunday of March to the last Sunday of October).

2.4. TELEPHONE NUMBER

+39 02 60843288

2.5. FACSIMILE NUMBER

None

2.6. OTHER TELECOMMUNICATION

None

2.7. ELECTRONIC MAIL ADDRESS

Nexi Payments CERT can be reached via cert@nexigroup.com

Messages sent to this address are received by all Nexi Payments CERT members.

2.8. PUBLIC KEYS AND ENCRYPTION INFORMATION

PGP/GnuPG is supported for secure communication. All members of Nexi Payments CERT have personal PGP key that use for exchange of information classified as “Restricted” or “Secret”, according to the Nexi Payments CERT Policy on Information Classification.

Nexi Payments CERT public PGP key for cert@nexigroup.com is available on the public keyservers.

2.9. TEAM MEMBERS

The list of team members will be published in the Nexi Payments CERT web portal (http://www.sia.eu/cert).

2.10. OTHER INFORMATION

None

2.11. POINTS OF CUSTOMER CONTACT

The preferred method for contacting Nexi Payments CERT is via e-mail: cert@nexigroup.com. The mailbox is monitored during regular office hours: Monday to Friday. 09.00-18.00. Except during public holidays in Italy.

If it is not possible or not advisable for security reasons to contact the Nexi Payments CERT via e-mail, contact may be made by telephone during regular office hours.

For security incidents use: cert@nexigroup.com

Please use PGP if you plan to send sensitive information.

3. CHARTER

3.1. MISSION STATEMENT

Nexi Payments CERT’s Computer Emergency Response Team for Nexi Payments Spa and its subsidiaries. The mission is to co-ordinate all activities aimed at the prevention, detection and response to cyber security incidents within its constituency.

3.2. CONSTITUENCY

The constituency of Nexi Payments CERT is the Nexi Payments S.p.A, its foreign and domestic subsidiaries, its business division and its services provided to the customers.

In particular Nexi Payments CERT is responsible for the follow ASN and IP adresses:

AS3269

AS12954

AS35051

AS208552

3.3. SPONSORSHIP AND/OR AFFILIATION

Nexi Payments CERT is managed by Nexi Payments S.p.A.

3.4. AUTHORITY

Nexi Payments CERT operates under the auspices of the Nexi Payments S.p.A.

4. POLICIES

4.1. TYPES OF INCIDENTS AND LEVEL OF SUPPORT

Nexi Payments CERT is authorized to address all types of cyber security incidents which occur, or threaten to occur, at its constituency (see 3.2). Nexi Payments CERT may act upon request of one of its constituents, or may act if a constituent is, or threatens to be, involved in a computer security incident. The level of support given by Nexi Payments CERT will vary according to the severity of the incident and the Nexi Payments CERT resources at the time.

Every effort will be done to give some response within two working day. Full and direct support is given to end user to ensure the full resolution of the incident.

Nexi Payments CERT is also committed to keeping its constituency informed of potential vulnerabilities, possibly before they are actively exploited.

4.2. CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

All incoming information is handled confidentially by Nexi Payments CERT, regardless of its priority. Information that is evidently very sensitive in nature is only communicated in encrypted format. When reporting an incident of very sensitive nature, please state so explicitly (e.g. by using the label SENSITIVE in the subject field of e-mail) and use encryption as well. Nexi Payments CERT will use the information you provide to help solve security incidents. This means explicitly that the information will be distributed further only on a need-to-know basis, and in anonymized fashion. If you have any particular concern regarding the information provided, please state explicitly what Nexi Payments CERT do with the information you provide. Nexi Payments CERT will adhere to your policy, but will also point out to you if that means that Nexi Payments CERT cannot act on the information provided.

We may advise owners of systems to report serious incidents to law enforcement. Nexi Payments CERT cooperates with law enforcement in the course of an official investigation only.

Nexi Payments CERT does not deal with the press directly. All press-enquiries will have to go via the communications office of Nexi Payments Spa.

4.3. COMMUNICATION AND AUTHENTICATION

Telephone and unencrypted e-mail are considered sufficient for the transmission of low-sensitivity data. Network file transfers will be considered similar to e-mail for these purposes. However we highly recommend using PGP/gpg to encrypt all information send to us via e-mail. We will use PGP/gpg whenever possible and view PGP/gpg signed and/or encrypted e-mail as an invitation to use PGP/gpg signing and encryption on return e-mail.
Nexi Payments CERT recognize and support the ISTLP (Information Sharing Traffic Light Protocol), following ENISA best practice.

5. SERVICES

5.1. INCIDENT RESPONSE (TRIAGE, COORDINATION AND RESOLUTION)

Nexi Payments CERT is responsible for the coordination of security incidents in our constituency and ensures that the incident are correctly handled and resolved. Nexi Payments CERT will provide assistance and support with respect to the following aspects of incident management:

5.1.1 INCIDENT TRIAGE

Incident triage is handled by Nexi Payments CERT. Events are analyzed by collecting all the information provided by the various technological sources and, therefore, categorized and prioritized. The priority level is assigned based on the strategic importance of information source (CEO, Top Management, LEAs, etc.), interest for the constituency (e.g. impact on services), the characteristics of the impacted systems (e.g. extension, criticality, etc.) and the legal impacts for the organization.

After categorization and prioritization of the event, before proceeding with its resolution, need of escalation is verified.

5.1.2 INCIDENT COORDINATION

Incident coordination is handled by Nexi Payments CERT, from the identification to its resolution.

Nexi Payments CERT analyze the incident, determining the root cause, prepare an incident report and inform and distribute information to constituency if necessary.

5.1.3 INCIDENT RESOLUTION

Incident resolution is coordinated by Nexi Payments CERT and is handled in cooperation with the involved constituents. In particular, Nexi Payments CERT defines and coordinates actions to contrast incidents and recovery activities designed to ensure a return to normal operations

(before the security incident) as quickly as possible. Such actions may include, for example, the reconnection of disconnected networks, the commissioning of services, systems or blocked applications, the restoring of corrupted or lost data backup. The return to normal operations is properly checked by specific tests on systems, applications and data. In case of failure new strategies are identified by Nexi Payments CERT.

Nexi Payments CERT provides adequate support and all the required details about the circumstances in which the incident occurred and the evidence on the individual or group of individuals responsible of the security incident.

5.2. PROACTIVE ACTIVITIES

Nexi Payments CERT performs the following proactive services for its constituency:

- Cyber Fraud Incident awareness
- Cyber Threat Intelligence & Analysis
- Security & Compliance Monitoring
- Vulnerability Handling

5.3. REACTIVE ACTIVITIES

Nexi Payments CERT performs the following reactive services for its constituency:

- Incident analysis
- Incident response support
- Incident response coordination
- Incident Handling
- Anti Malware – Artifact handling
- Incident Forensic

6. INCIDENT REPORTING FORMS

A standard incident reporting form is available from http://www.sia.eu/cert. It is also possible to report security incidents via encrypted e-mail to cert@nexigroup.com
When reporting incidents, please provide as much information as possible.

For example:

- Contact details and organization information (name or person, name or organization, address)
- Type of incident (malicious code, compromised systems, information gathering, etc.)
- Time and date of all events reported. Also include in which time zone the events were reported or detected. This will help us to correlate your information with ongoing incidents.
- If it's regarding malicious code please contact us by email before to agree on a transfer mechanism avoiding problems with network based anti-virus tools and intrusion detection systems.
- Level of urgency

- Please classify the information using the Traffic Light Protocol and make sure to always include your own contact information

In addition Nexi Payments CERT implement an internal ticketing system available to its constituency through the company intranet.

7. DISCLAIMERS

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