RFC 2350 - CERT Nomios

Version 2.1 - Published - 2026-08-31

Classification	**TLP: CLEAR / PUBLIC**
Owner	CERT Nomios
Scope	Public RFC 2350 information for CERT Nomios.
Language	English
Status	Published

Purpose: This TLP:CLEAR document provides public RFC 2350 information about CERT Nomios: identity, constituency, authority, contact channels, information handling and high-level services. CERT Nomios supports Nomios Group and organizations using CERT Nomios services. Commercial terms, detailed capabilities and service levels are not covered by this public document.

Version History

Version	Date	Author	Nature of modification
1.0	2025-12-09	CSIRT Nomios	Initial internal version.
2.0	2026-03-18	CERT Nomios	Reworked structure for the CSIRT to CERT migration
2.1	2026-08-31	CERT Nomios	Refocused the document as a concise public RFC2350 profile for a managed CERT capability serving both Nomios Group and eligible customers.

1. Document Information

Date of last update	Version 2.1, published on 2026-08-31.
Distribution list for notifications	Notifications of updates may be sent to registered customers, trusted partners and relevant CSIRT/CERT contacts upon request.
Locations where this document may be found	The latest approved TLP:CLEAR version is published on the Nomios website, on the CERT / incident response page.
Authenticating this document	A signed version of this document may be provided using the CERT Nomios PGP key.
Document identification	Title: RFC 2350 - CERT Nomios Public Identity Profile Version: 2.1 Status: Published Classification: TLP:CLEAR Expiration: This document remains valid until superseded by a later version.

2. Contact Information

Name of the team	Official name: CERT Nomios Short name: CERT Nomios
Address	Nomios SAS, 64 avenue Jean-Baptiste Clément, 92100 Boulogne-Billancourt, France
Time zone	Europe/Paris. Standard time UTC+1; daylight saving time UTC+2 when applicable.
Telephone number	+33 (0)1 41 10 28 48 - NOMIOS France Support
Facsimile number	Not applicable.
Other telecommunication	Secure transfer mechanisms may be established during an investigation, including secure portal, encrypted exchange or SFTP where appropriate.
Electronic mail address	For information security incident notifications, contact: cert@nomios.fr
Public keys and encryption information	PGP key fingerprint: 11B9 E3B1 A945 07DB 9A17 A95A 0384 C35A 740C 06C9 Key retrieval: https://keys.openpgp.org/vks/v1/by-fingerprint/11B9E3B1A94507DB9A17A95A0384C35A740C06C9
Team members	Head of CERT: Kevin BERTRAND Individual team members are not publicly listed. A CERT lead or incident coordinator is assigned as point of contact during engagements.
Other information	Additional information about Nomios services is available at https://www.nomios.fr/cert and through customer account teams.
Points of customer contact	Preferred reporting channels: cert@nomios.fr, Nomios support portal and Nomios web contact form. Registered customers may use their dedicated communication channel.
Hours of operation	CERT Nomios can be contacted at any time through the channels listed in this document. Service availability and response commitments depend on the applicable customer agreement or internal governance model.
Preferred languages	French and English.

3. Charter

3.1 Mission Statement

CERT Nomios is a managed CERT capability operated by Nomios Group. It operates as the CERT capability for Nomios Group and as a managed incident response and coordination service for eligible customers.

Its mission is to provide a trusted point of contact for cybersecurity incident reporting, coordination, information exchange and response support within its defined constituency.

3.2 Constituency

- Internal constituency: Nomios Group information systems and entities.
- Customer constituency: organizations using CERT Nomios services under an applicable agreement or mandate.
- External interaction: peer CERT/CSIRT teams, trusted security communities, authorities, vendors and partners when coordination is authorized or required.
- Product scope: Vulnerability reports concerning Nomios-owned information systems may be received and coordinated by CERT Nomios. Reports regarding third-party products are redirected to the appropriate vendor or PSIRT.

3.3 Sponsorship, Affiliation and Governance

CERT Nomios is part of Nomios Group, a European cybersecurity and networking services provider. It may coordinate with internal Nomios teams or trusted external parties when required and authorized.

Nomios Managed Services operate under an ISO 27001 certified Information Security Management System. This statement does not imply that CERT Nomios itself is a separately certified external CERT unless explicitly stated in future versions.

3.4 Authority

For Nomios Group information systems, CERT Nomios operates under Nomios internal governance. For customer engagements, CERT Nomios acts under the authority granted by the customer through the applicable mandate or agreement.

CERT Nomios does not take operational action on third-party systems without authorization from the responsible organization.

4. Policies

4.1 Incident Types and Level of Support

CERT Nomios handles or coordinates cybersecurity incidents affecting its constituency. The level of support depends on the nature of the incident, the affected constituency and the applicable mandate.

4.2 Co-operation, Interaction and Disclosure of Information

CERT Nomios may cooperate with peer CERT/CSIRT teams, authorities, vendors and trusted partners when necessary for incident handling and permitted by applicable laws, mandate and confidentiality requirements.

Information sharing follows the Traffic Light Protocol and the need-to-know principle. Customer identity, evidence, indicators, investigation details and business impact information are not disclosed externally without authorization, unless disclosure is legally required.

CERT Nomios may participate in trusted cybersecurity communities and information-sharing groups.

4.3 Communication and Authentication

The preferred communication methods are the Nomios support portal and email at cert@nomios.fr. Sensitive information should be exchanged using PGP encryption, an approved secure portal, SFTP or another mutually agreed secure mechanism. Identity verification and communication channels may be reinforced during critical incidents. Registered customers have a dedicated communication channel.

4.4 Data Protection, Evidence Handling and Confidentiality

- Incident-related information is treated as sensitive by default.
- Access is restricted to authorized personnel on a need-to-know basis.
- Evidence and personal data are handled according to applicable legal, contractual and confidentiality requirements.
- Customer-sensitive information is not shared externally without authorization, unless legally required.

5. Services

CERT Nomios provides:

- Incident intake and triage
- Incident coordination
- Incident response support
- Threat intelligence sharing
- Security advisory services
- Crisis communication support when applicable

6. Incident Reporting

6.1 Reporting Channels

- Email: cert@nomios.fr. PGP encryption is recommended for sensitive incident information.
- Support portal: https://support.nomios.fr/
- Nomios website contact form: https://www.nomios.fr/contact/
- Telephone: +33 (0)1 41 10 28 48.

6.2 Required Information

When reporting an incident, provide the following information when available:

- Reporter identity, organization and contact details.
- Summary of the incident and affected organization, systems or services.
- Relevant dates, indicators, evidence or alerts.
- Actions already taken and any urgent constraints.