UniCredit

RFC2350 Profile

UNICREDIT COMPUTER EMERGENCY RESPONSE TEAM **(UNT-CERT)**

April 17, 2023

Table of Contents

This document contains a brief description of the "UniCredit Computer Emergency Response Team (UNT-CERT)", in accordance with RFC2350 specification.

1 Document Information

1.1 Date of Last Update
This is version v1.6, published April 17, 2023.

1.2 Distribution List for Notifications
There is no distribution list to notify changes in this document.

1.3 Locations where this Document May Be Found
The current and latest version of this document can be found at: https://www.unicreditgroup.eu/cert
Please make sure you are using the latest version.

2 Contact Information

2.1 Name of the Team
Full name: UniCredit Computer Emergency Response Team.
Short name: UNT-CERT.

2.2 Address
UniCredit
CERT
Via Livio Cambi, 1
20151, Milano
Italy.

2.3 Time Zone
Central Europe, (GMT+1 and GMT+2 from the last Sunday of March to the last Sunday of October).

2.4 Telephone Number
+39 02 00706830 (operating 24H/7D all year round).

2.5 Facsimile (Fax) Number
None available.

2.6 Other Telecommunication
None available.

2.7 Electronic Mail Address
cert [at] unicredit [dot] eu

2.8 Public Keys and Encryption Information
UNT-CERT supports PGP/GnuPG encryption for secure communication.
All members of UNT-CERT have personal PGP keys that can be used for exchange of classified information.
UNT-CERT team latest public PGP key is available on public keyservers and at the following address:
https://www.unicreditgroup.eu/cert

2.9 Team Members
Undisclosed information.

2.10 Other Information
None available.

2.11 Points of Customer Contact
The preferred method for contacting UNT-CERT is via the e-mail mentioned in §2.7.
In case of urgency and/or emergencies, or when a contact via e-mail is not possibile/advisable, the telephone number mentioned in §2.4 operates 24H/7D all year round.

3 Charter

3.1 Mission Statement
UNT-CERT mission is to provide assistance to UniCredit Group's served legal entities, regarding ICT security incident assessment, handling, analysis and response.

Main activities are:

- Cyber attack management and IT incident response, analyzing ICT security incidents and identifying countermeasures to address the necessary mitigation;
- Major incident management, with the coordination of the various company functions involved and the preparation of appropriate reporting;
- Conduction of investigations using forensic analysis techniques in order to manage ICT security incidents by providing reactive services (incident responses) and a complete portfolio of other security services, such as monitoring improvement, early warning and malware analysis.

UNT-CERT ensures cooperation within national and international networks of CSIRTs/CERTs.
UNT-CERT supports law enforcement and regulatory authorities regarding ICT security incidents.

3.2 Constituency
UNT-CERT constituency refers to UniCredit Group's served legal entities (https://www.unicreditgroup.eu), their relevant assets, services and Customers.

3.3 Affiliation
UNT-CERT is part of the UniCredit Group.

3.4 Authority
UNT-CERT operates under the auspices of, and with authority delegated by UniCredit Group.

4 Policies

4.1 Types of Incidents and Level of Support
UNT-CERT is responsible for addressing all types of ICT security incidents occurring within its constituency, as defined in §3.2.
Internal use only policies regulate CERT's goals, responsibilities and roles.

4.2 Co-operation, Interaction and Disclosure of Information

While there are legal, regulatory (e.g., GDPR), ethical and internal restrictions on the flow of information, UNT-CERT highly regards the importance of technical and operational cooperation and information sharing among CSIRTs/CERTs, with whom a relationship of mutual trust has been established, or belonging to the same trust networks.

This Co-operation includes the exchange of information regarding ICT security incidents and vulnerabilities, exclusively from a technical standpoint and always without references to any security incident occurred within UniCredit Group's perimeter, past and present.

Therefore, while appropriate measures will be taken to protect the identity of members of our constituency, personally identifiable information (PII), data and security measures applied on UniCredit Group's perimeter, UNT-CERT will share information when this assists others in resolving or preventing security incidents.

4.3 Communication and Authentication

The preferred method for contacting UNT-CERT is via the e-mail mentioned in §2.7. The alternative contacting method is via the telephone number mentioned in §2.4, operating 24H/7D all year round.

Telephone and unencrypted e-mail are are considered reasonably safe channels in order to share unsensitive/low-sensitive data.

Usage of Information Sharing Traffic Light Protocol (ISTLP) is advised.

We strongly suggest encrypting all sensitive communication sent to the UNT-CERT with our latest public PGP key, detailed in §2.8, in such a way as to guarantee the confidentiality of the information shared.

5 Services

5.1 Incident Response

UNT-CERT is in charge of the "ICT Security Incident Response" activity, which is part of the sub-process of ICT Security Incident Handling, inside the ICT Security Incident Management process.

In particular, UNT-CERT performs the main sub-activities of:

- Containment
- Eradication
- Recovery

The ICT Security Incident Response is the main activity performed to contain and limit damage from the ICT Security Incident, minimize impact on business operations of the Legal entity, define response and act accordingly to recover from the effects of the ICT Security Incident. This activity involves further analysis of available information to understand the business impact, required resolution tasks and whether the same incident may have happened in or affected other systems, or the same vulnerability can be immediately exploited by malicious party in other systems, parts of the infrastructure or network. In this case, additional tasks to mitigate the information security threat shall be designed and planned.

All actions and all decisions taken in the course of the Incident Handling must be documented.
UNT-CERT provides ICT Security Incident coordination, facilitating communication among involved stakeholders.

UNT-CERT is also responsible for ICT Security Incident resolution, ensuring the determination of the root cause.

5.2 Proactive Services

UNT-CERT provides the following proactive services for its constituency:

- Security assessments
- Evaluation of security tools
- Intrusion detection services

5.3 Reactive Services

UNT-CERT provides the following reactive services for its constituency:

- Alerts and warnings
- Incident handling
- Incident analysis
- Incident response on site
- Incident response support
- Incident coordination
- Vulnerability analysis
- Vulnerability response
- Artifact handling
- Artifact analysis
- Artifact response
- Artifact coordination
- Forensic analysis

5.4 Quality Services

UNT-CERT provides the following quality services for its constituency:

- Risk analysis
- Security consulting
- Product evaluation

6 Incident Reporting Forms

There is no defined template of form for reporting incidents to UNT-CERT. Nevertheless, incident notification can be done via the email mentioned in §2.7.

7 Disclaimer

While every reasonable precaution has been taken in account, UNT-CERT assumes no responsibility for any error or omission, or for damages resulting from the use or misuse of the information contained herein.