TLP: WHITE

ALTER CERT

RFC 2350

DECEMBER 11, 2023

6 Av. Du Général de Gaulle, 78000 Versailles, France

ALTERSOLUTIONS

act digital group

Contents

1. Document information 3
1.1. Date of last update 3
1.2. Distribution list 3
1.3. Locations where this document may be found 3
1.4. Authenticating this document 3
1.5. Document identification 3
2. Contact information 4
2.1. Name of the team 4
2.2. Address 4
2.3. Time zone 4
2.4. Telephone Number 4
2.5. Facsimile Number 4
2.6. Other means for communication 4
2.7. Electronic mail address 5
2.8. Public keys and other encryption information 5
2.9. Team member 5
2.10. Other information 5
2.11. Points of customer contact 5
3. Charter 6
3.1. Mission statement 6
3.2. Constituency 6
3.3. Sponsorship and/or affiliation 7
3.4. Authority 7
4. Policies 8
4.1. Type of incident and level of support 8
4.2. Co-operation, interaction, and disclosure of information 8
4.2.1. Co-operation and Interaction: 8
4.2.2. Disclosure of Information: 9
4.3. Communication and Authentication 9
5. Services 10
5.1. Incident response 10

5.1.1. Incident triage 10
5.1.2. Incident coordination 10
5.1.3. Incident resolution 10
5.2. Proactive activities 10
5.2.4. Intrusion detection services 10
5.2.5. Incident response planning and drills 11
5.2.6. Vulnerability management 11
6. Incident reporting forms 12
7. Disclaimers 13

1. Document information

This document contains a description of ALTER CERT according to RFC2350.

It provides basic information about the ALTER CERT team, its channels of communication, roles, and responsibilities.

1.1. Date of last update

Version 1.0 – 2023/12/11

1.2. Distribution list

There is no distribution list for notifications.

1.3. Locations where this document may be found

The current and latest version of this document is available from the Alter Solutions website: https://www.alter-solutions.com/alter-cert_rfc2350

1.4. Authenticating this document

This document has been signed with the PGP key of ALTER CERT.

The signature of this document is available at: https://5690371.fs1.hubspotusercontent-na1.net/hubfs/5690371/ALTER-CERT_RFC2350.pdf.sig

1.5. Document identification

Title: ALTER CERT – RFC 2350

Version: 1.0

Document date: 2023/12/08

Expiration: This document is valid until superseded by a later version.

2. Contact information

2.1. Name of the team

Alter CERT

Alter CERT is Alter Solutions commercial and internal CERT.

2.2. Address

Alter CERT

6 Avenue du Général de Gaulle

78000 Versailles

France

2.3. Time zone

CET / CEST – Paris time

2.4. Telephone Number

+33 1 87 66 97 36

2.5. Facsimile Number

None.

2.6. Other means for communication

None.

2.7. Electronic mail address

If you need to notify us about an information security incident or a cyber-threat targeting or involving your company or Alter Solutions, please contact us at cert@alter-solutions.com.

This is a mail monitored by the person(s) on duty for the ALTER CERT.

2.8. Public keys and other encryption information

Alter CERT has a PGP public key available at https://keys.openpgp.org

ID: 9DE1AB3C2DDDFF7B333E543262059FB543DD8F6B

2.9. Team member

Nabil DIAB is the current Alter CERT team leader. The team consists of IT security analysts.

The list is not publicly available.

2.10. Other information

None.

2.11. Points of customer contact

The preferred method to contact Alter CERT team is to send an email to the cert@alter-solutions.com address, which is monitored during hours of operation.

Urgent cases can be reporter by phone on +33 1 87 66 97 36.

Days / hours of Operations: 09:00 to 23:00, Monday to Friday.

Customer can contact Alter CERT outside of office hours of operations through special on-call phone number which is not publicly disclosed.

3. Charter

3.1. Mission statement

Our mission at Alter CERT is to provide robust and responsive cybersecurity incident response services, safeguarding the digital assets and operations of our internal stakeholders as well as our diverse client base. We are dedicated to delivering expert guidance, timely intervention, and comprehensive solutions to manage and mitigate cyber threats.

As a trusted authority in the cybersecurity domain, we strive to:

- **Enhance Cyber Resilience**: Proactively fortify the cybersecurity posture of our clients through cutting-edge technologies, best practices, and continuous awareness.
- **Rapid Incident Response**: Offer swift and efficient response to cybersecurity incidents, minimizing impact and guiding recovery efforts.
- **Expertise and Excellence**: Maintain the highest standards of technical expertise and operational excellence in all facets of cybersecurity incident handling.
- **Collaboration and Communication**: Foster strong partnerships with industry peers, law enforcement, and cybersecurity communities to stay ahead of evolving cyber threats.
- **Education and Awareness**: Empower our clients and the wider community through education, sharing insights, and promoting cybersecurity awareness.

In executing our mission, we adhere to principles of integrity, confidentiality, and relentless commitment to cybersecurity, ensuring a safer digital environment for all our stakeholders.

3.2. Constituency

The constituency of Alter CERT is primarily centered around two key groups:

- **Internal Constituency - Alter Solutions Group**: This includes all departments, branches, and entities within the Alter Solutions group. Our services cover every aspect of our internal network, digital resources, and operations.

- **External Constituency - Commercial Clients**: Alongside our internal focus, Alter CERT extends its expertise to a wide array of external clients. These clients, who engage our services for cybersecurity needs, benefit from clearly defined Service Level Agreements (SLAs). Our SLAs detail the expected response times, availability of our team, the scope of incident response services offered, and any other specific commitments or standards we uphold in our service delivery.

3.3. Sponsorship and/or affiliation

Alter CERT is part of Alter Solutions company: https://alter-solutions.com

3.4. Authority

For internal matters, Alter CERT operates under the authority of the CEO of Alter Solutions.

For external incidents, Alter CERT coordinates security incident on behalf of its constituency, and only at its constituent's request.

4. Policies

4.1. Type of incident and level of support

At Alter CERT, our expertise encompasses a wide array of cybersecurity incidents, reflecting the diverse and evolving landscape of cyber threats. Our team is equipped to manage various types of incidents, tailored to the unique challenges presented in each situation.

- **Types of Incidents**: Our capabilities enable us to handle all types if computer security incidents which occur or threaten to occur in our constituency. We are prepared to address incidents that impact the confidentiality, integrity, and availability of information and systems, both for our internal operations within the Alter Solutions group and for our external clients.
- **Level of Support**: The level of support provided by Alter CERT is determined based on several parameters, including the severity of the incident, the potential impact on the affected entity, the complexity of the required response, and the urgency of the situation. Our response is scalable and adaptable, ensuring that each incident is met with an appropriate and effective level of support.

This flexible approach allows us to offer a range of responses, from advisory and guidance for lower-severity incidents to comprehensive, hands-on involvement for more severe or complex situations. Our priority is to provide a responsive, effective, and tailored approach to each cybersecurity incident, ensuring the best possible outcome for our stakeholders.

4.2. Co-operation, interaction, and disclosure of information

4.2.1. Co-operation and Interaction:

- **With Internal Teams and Departments**: Alter CERT actively collaborates with various internal departments within the Alter Solutions group. This includes sharing information, coordinating responses, and providing mutual support to enhance overall cybersecurity posture.
- **With External Entities**: Our team engages in collaboration with external organizations, including other CERTs, cybersecurity experts, industry groups,

and law enforcement agencies. These interactions aim to foster a collective defense against cyber threats, sharing insights, trends, and best practices.

- **Participation in Industry Forums and Events**: We regularly participate in cybersecurity forums, conferences, and workshops. This involvement not only keeps us abreast of the latest developments in cybersecurity but also allows us to contribute to the broader community.

4.2.2. Disclosure of Information:

- **Confidentiality and Privacy**: Alter CERT adheres strictly to confidentiality and privacy standards. Sensitive information, particularly that which pertains to specific incidents or clients, is handled with the utmost discretion and in accordance with applicable laws and regulations.
- **Information Sharing Protocols**: We have established protocols for sharing information that balance the need for openness with the requirement to protect sensitive data. This includes anonymizing data where necessary and ensuring that any shared information does not compromise the security of affected parties.
- **Legal and Regulatory Compliance**: All disclosures and information sharing are conducted in compliance with relevant legal and regulatory frameworks. This ensures that our actions are not only effective in combating cybersecurity threats but also lawful and ethically sound.
- **Incident Reporting**: In cases where incidents have broader implications or require external intervention, Alter CERT follows established procedures for reporting these incidents to appropriate authorities and stakeholders in a timely and responsible manner.

4.3. Communication and Authentication

For normal communication without any sensitive information, unencrypted e-mail may be used but Alter CERT strongly encourage customers to use encrypted and signed e-mail using PGP to exchange data.

5. Services

5.1. Incident response

5.1.1. Incident triage

The process of receiving, evaluating, and prioritizing incoming incident reports. This step involves initial assessment to determine the scope, severity, and potential impact of the incident.

5.1.2. Incident coordination

Facilitating the response to incidents by coordinating between different stakeholders, which may include internal teams, external clients, and other relevant parties. This involves communication, resource allocation, and strategy implementation.

5.1.3. Incident resolution

Direct involvement in resolving the incident, which includes containment, eradication of the threat, recovery of affected systems, and providing detailed advice for preventing future occurrences.

5.2. Proactive activities

5.2.4. Intrusion detection services

Continuous monitoring and analysis of systems and networks to detect and alert on signs of unauthorized access or malicious activities.

5.2.5. Incident response planning and drills

Helping organizations to develop and test their incident response plans through table-top exercises or simulated incident scenarios, to ensure they are prepared for real-world incidents.

5.2.6. Vulnerability management

Identifying, evaluating, and advising on vulnerabilities within systems and software. This involves regular scanning, assessment of potential impact, and recommendations for mitigation.

6. Incident reporting forms

Please report security incidents via encrypted email to cert@alter-solutions.com.

We provide the following assessment table as a flexible guide to help our client frame their request for incident response services. This table is designed to capture critical information that will assist us in understanding and prioritizing the incident. It is not a strict form; rather, it serves to ensure that we receive the essential details necessary to initiate an effective response. Please provide as much information as possible in each category, and feel free to include any additional relevant details that may support the assessment and subsequent handling of your cybersecurity incident.

Category	Information	Assessment
Timestamps	Time of the first observed malicious activity	Record the exact date time when the incident was first observed and when it was reported.
Incident details	Nature of the Incident	Describe the nature of the incident, including what happened and how it was discovered.
Affected systems	Asset Name, Type and Function	List the names, types, and functions of all systems impacted by the incident.
	Asset IP and Network Range	Provide the IP addresses and network ranges of the affected assets.
	Asset Criticality	Assess the criticality of each affected asset to your operations.
	Asset owner / Department	Identify the department or individual who owns each affected system.
Network details	Port and Protocol involved	Note the network ports and protocols involved in the incident.
User details	Account Names	Include the names of any user accounts that were active or compromised during the incident.
Other	Other relevant details	Include any additional information that could be relevant to the incident, such as unusual system behavior observed, relevant recent changes to the system or network, or any other observations that do not fit the categories above but may aid in the investigation.

Table 1 - Incident assessment table

7. Disclaimers

While we strive to ensure the accuracy and relevance of the information, Alter CERT makes no warranties of any kind, whether expressed or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the document or the information, services, or related graphics contained herein for any purpose. Any reliance placed on such information is therefore strictly at the user's own risk.