RFC 2350

Oneconsult International Computer Security Team (OCINT-CSIRT)

1 June 2024

VERSION	1.0
CLASSIFICATION	TLP:CLEAR

Oneconsult International AG
c/o OCINT-CSIRT
Giesshübelstrasse 45
8045 Zürich
Switzerland

Table of Contents

Version	Date	Description	Author
1.0	2024-06-01	Initial Publication	Gregor Wegberg

1. Document Information

This document, following RFC 2350[1] (Expectations for Computer Security Incident Response), provides a summary of basic information about the commercial and internal OCINT-CSIRT of Oneconsult International AG. In particular contact options, who belongs to the constituency and how to notify OCINT-CSIRT about incidents, as well as information about its role and services offered.

1.1 Date of Last Update

This document is Version 1.0, published on 2024-06-01.

This document is valid until superseded by a later version.

1.2 Distribution List for Notifications

Changes to this document are distributed solely internally within Oneconsult International AG using the current internal communication recommendations. Hence there is no public distribution list for notifications.

This document is kept up to date at the location specified in chapter 1.3. Should you have any questions regarding changes to this document, please reach out to OCINT-CSIRT using one of the communication channels listed in chapter 2.

1.3 Locations where this Document May Be Found

The current and latest version of this document is available online under the following URL:

https://www.oneconsult.com/en/rfc2350/

You can request the current and latest version of the document through contacting OCINT-CSIRT using one of the communication channels listed in chapter 2.

1.4 Authenticating this Document

This document has been digitally signed by Tobias Ellenberger, CEO of Oneconsult International AG, and Gregor Wegberg, Head of Digital Forensics & Incident Response.

[1] https://www.ietf.org/rfc/rfc2350.txt

2. Contact Information

2.1 Name of the Team

- Short Name: OCINT-CSIRT
- Full Name: Oneconsult International Computer Security Incident Response Team

2.2 Address

Oneconsult AG

c/o OCINT-CSIRT

Giesshübelstrasse 45

8045 Zürich

Switzerland

2.3 Time Zone

OCINT-CSIRT is located in the central European time zone (CET/CEST) which is GMT+0100 (CET) and GMT+0200 during daylight saving time (CEST).

2.4 Telephone Number

An on-call phone number is available 24/7, restricted to the internal constituency and to commercial entities with an SLA agreement.

All other constituents can reach OCINT-CSIRT during office hours (except for Swiss national and local holidays in Zurich, Switzerland) from 08:00 to 18:00 CET/CEST under the following telephone number: +41 43 377 22 90.

2.5 Other Telecommunication

No other telecommunication channels are available.

2.6 Electronic Mail Address

OCINT-CSIRT can be reached at csirt@oneconsult.com.

2.7 Public Keys and Encryption Information

OCINT-CSIRT PGP Key Information:

- User ID: `Computer Security Incident Response Team <csirt@oneconsult.com>`
- Key ID: `20FEB3447CD5C52C`
- PGP Fingerprint: `313B40ED7DA622AEB9C8DDC620FEB3447CD5C52C`

The public key is available at least at the following locations:

- In this document in chapter 9.1
- It can be retrieved from https://securemail.oneconsult.com/ (use the Search and search for the e-mail address mentioned under chapter 2.6)
- From the FIRST team page[2]

2.8 Team Members

The OCINT-CSIRT is a virtual team within Oneconsult International AG. It consists of the Digital Forensics and Incident Response (DFIR) Teams in Switzerland and Germany as well as specially trained and qualified employees of Oneconsult AG, Oneconsult Deutschland AG, and Oneconsult New Zealand Limited.

2.9 Other Information

The preferred language for communication is German or English. OCINT-CSIRT can also communicate in French and Italian.

Requests for additional information can be sent to the e-mail address listed under chapter 2.6.

2.10 Points of Customer Contact

In case of emergency OCINT-CSIRT should be contacted by telephone (see chapter 2.4). For other enquiries the listed phone number (see chapter 2.4) or e-mail address should be used (see chapter 2.6).

[2] https://www.first.org/members/teams/ocint-csirt

3. Charter

3.1 Mission Statement

The Oneconsult International Computer Security Incident Response Team (OCINT-CSIRT) is Oneconsult's CSIRT, established to make cyberspace safer. The OCINT-CSIRT is the point of contact for Oneconsult's existing and future customers, as well as for the Oneconsult International AG and its subsidiaries. Its services focus on preparing its constituency to deal with information security events and incidents and assisting them in responding to information security incidents of all kinds.

3.2 Constituency

OCINT-CSIRT is operated by Oneconsult with its own staff and provides services to Oneconsult customers as a commercial CSIRT and to Oneconsult International AG with its subsidiaries as an internal CSIRT. The OCINT-CSIRT consists of permanent members of the DFIR team in Switzerland and Germany. It can be augmented by Oneconsult employees from other units as needed to fulfil its mission.

3.3 Sponsorship and/or Affiliation

OCINT-CSIRT is fully sponsored, operated, and supported by Oneconsult International AG with its subsidiaries.

It maintains contacts with various national and international CSIRTs and CERTs; commercial and internal CSIRTs and CERTs; national and international authorities; national and international law enforcement agencies; and other non-governmental organizations, communities, associations, and similar organizations.

3.4 Authority

During information security incidents, the OCINT-CSIRT analyses, investigates, advises, assists, supports, and coordinates security incidents affecting its constituency. The OCINT-CSIRT does not have the authority to act on its own without the approval of an entity with the necessary authority within the affected organization or by following a preapproved playbook/process.

Outside of information security incidents, the OCINT-CSIRT may be invited by its constituents to prepare for incidents, conduct exercises to train for incidents, lead or participate in lessons learned to improve their cyber resilience, and share its expertise with organizations on appropriate occasions to reduce the likelihood and impact of information security incidents.

4. Policies

4.1 Types of Incidents and Level of Support

Incidents are prioritised according to contract status, type and therefore the service level agreed with the affected constituent. Incidents affecting constituents without a Service Level Agreement (Incident Response Retainer) will be prioritised according to the severity of the incident, the nature of the organisation affected and in accordance with the resources available to ensure the contractual service levels are met.

4.2 Co-operation, Interaction and Disclosure of Information

OCINT-CSIRT aims to share actionable information with other entities in order to fulfil its mission (see chapter 3.1), in particular with the entities mentioned in chapter 3.3, and within the contractual and legal constraints. OCINT-CSIRT operates within the current Swiss and German legal framework.

All requests to OCINT-CSIRT are treated with due care. OCINT-CSIRT adheres to the latest version of the Traffic Light Protocol (TLP) as defined by FIRST[3]. Written messages and documents should be clearly tagged with a TLP label. In case of a contact by phone, video conference or similar, the TLP classification should be stated prior to the delivery of the information. If not stated otherwise, OCINT-CSIRT asks for a TLP classification. In cases where this is not possible, OCINT-CSIRT defaults to TLP:AMBER+STRICT as defined by TLP version 2.0.

It is recommended to encrypt digitally transferred sensitive information, e.g. with the PGP key mentioned in chapter 2.7 or using end-to-end encryption. On request, OCINT-CSIRT can provide an encrypted communication and data exchange channel or platform.

4.3 Communication and Authentication

To ensure authenticity and confidentiality of information use PGP signatures and encryption (see chapter 2.7) or other agreed upon signing and encryption methods.

[3] https://www.first.org/tlp/

5. Services

Services are described based on the definition of the FIRST CSIRT Services Framework[4] in version 2.1.

5.1 Information Security Event Management

Within the Information Security Incident Management service area, OCINT-CSIRT provides temporary resources and second opinions to assist SOCs, CDCs and CSIRTs with monitoring and detection, and event analysis.

For some constituents, the OCINT-CSIRT is the primary or secondary contact for the constituent's monitoring and/or detection team for event analysis.

5.2 Information Security Incident Management

Information Security Incident Management services is one of the primary service areas of OCINT-CISRT. OCINT-CSIRT provides the full spectrum of information security incident report acceptance, information security incident analysis, artifact and forensic evidence analysis, information security incident coordination, mitigation and recovery, and crisis management support. Depending on the affected constituent the following parts of the listed services (functions) are provided with subject matter experts from partner companies:

- Implementing ad hoc measures and containment as well as system restoration
- Media communication
- Legal support (Note: This is not a service within the FIRST CSIRT Service Framework, but it is an important aspect of OCINT-CSIRT's work and is therefore mentioned here)

5.3 Vulnerability Management

OCINT-CSIRT is responsible for vulnerability report intake for Oneconsult International AG and its subsidiaries (internal CSIRT). These services are provided to commercial customers of Oneconsult International AG and its subsidiaries by the Penetration Testing & Red Teaming unit.

The following vulnerability management services are provided internally and for commercial customers by the Penetration Testing & Red Teaming unit, and the Research & Innovation unit:

- Vulnerability discovery / research
- Vulnerability analysis
- Vulnerability disclosure
- Vulnerability coordination
- Vulnerability response

5.4 Situational Awareness

Situational awareness services are provided by OCINT-CSIRT in cooperation with Oneconsult International AG Penetration Testing & Red Teaming, the Security Consulting, and the Research and Innovation units to its constituents. This includes the services data acquisition, analysis and synthesis, and communication.

[4] https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

5.5 Knowledge Transfer

OCINT-CSIRT focuses on and is responsible for providing exercises to its constituents. General information security awareness building, and training and education services are provided through the Cyber Security Academy unit within Oneconsult International AG. DFIR specific awareness building and training is provided and performed by the OCINT-CSIRT. Technical and policy advisory services are provided by the Security Consulting unit within Oneconsult International AG in cooperation with OCINT-CSIRT.

6. Incident Reporting Forms

There are no forms available. The preferred way of reporting incidents is by telephone (see chapter 2.4).

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, OCINT-CSIRT CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

8. Signatures

Oneconsult AG

Tobias Ellenberger
CEO Oneconsult Group
8045 Zürich, 02.06.2024

FES Fortgeschrittene elektronische Signatur
Signiert auf Skribble.com

Tobias Ellenberger

CEO Oneconsult International AG

Oneconsult AG

Head of Digital Forensics & Incident Response
Oneconsult AG, 01/06/2024

AES Advanced electronic signature
Signed on Skribble.com

Gregor Wegberg

Head of Digital Forensics & Incident Response

9. Appendix

9.1 PGP Public Key for csirt@oneconsult.com

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFyKEsQBEAC3YDVYLdLGEvEwOqM+UqDOtEroLxMdFy35a+UprcsknkBrrF76
NIGqxMYPO/re5v5yR6S9d9OHEjra8EaiY0iKmSSsRL4LuGrYzvmLmBOWgPdM1pZE
Z2m0aUkZA1io44IgTfGJtHNrX3EdpVRBmBe4HQ4fPJMaOjPHmmrFGRmzDK/nSXBw
Yz7FJ39KPn84MetlPNUoyc5SPRCXw9HcNjRxlDhzAHX5a08YqXw8S+kwt0CmdZIz
sUcq3MgfN2No5v7m24Sop76L6EKcHXG94h5xbeczn XwKHZqENkf+tvSI27G9kv8i
7orfMQBWSEm66zt/m7RQ1qLFNiDnqujMqgeqsE9IWM2zHu0NUHBDkALvdch55AHa
Jkq8YlxNi3HfjW3vDO5nLvWSanvpjDTaEK/HjxRwMOHCp3lEDZ1MzSTBA1o91Mjx
gF6mTHfHwSFf6MGGTY02ugGQ3TAmko/AMwmhPl3prO5RywzzJJd1T++139jSG0rY
BIuRIn/sGsHW5L0B0RaYsrr7dAEUAfst5O9McLdGttegiCq8WHFqwr+bR3ZqYWhB
6zm59F60k98Dq3aAZooFz3pZbNc3cKEw5ZE8LwdVJPBU9GQUpaPnZpSiMuye/kd8
SUZwuaoKfWY1TiDjrWEgJIoFqMjiBkHu2Nr3O9Uz+0eYKjt0Mvf1i4N/5QARAQAB
tD9Db21wdXRlciBTZWN1cml0eSBJbmNpZGVudCBSZXNwb25zZSBUZWFtIDxjc2ly
dEBvbmVjb25zdWx0LmNvbT6JAj4EEwECACgFAlyKEsQCGwMFCRLLe6wGCwkIBwMC
BhUIAgkKCwQWAgMBAh4BAheAAAoJECD+s0R81cUsN7oP/i1zzt9ij2PqEAKMdbHW
FEFERMOwVr+92RE03S8uJthbUj23L2EFA8jfTpJosdAl6HX4ydiPdq4EFQoER/ID
r8ry8t3J9MH4n1aUz8v9EfxFBBDHX5/KBfNxqumPngsRuEwhYw6E3o2tZRWF10jw
XfCkWoZFgurXRW7lGPwIBrc9SE2LHOh9fjDzIkm7hdTBlHf3uge0oBHBVFJZ21eM
HqkuFt0thS/5NLvch7mH5mi/RYvjWl43HIkQdjcWp1+m1jZkoK86qkjGI/rzhb+U
Gzl9PQMC/8zh4EpUQeXytBJ5KkuXJ6gjmhobRZWlCw3/gp9C+3kBI4n+vPLQWZnk
DvBaMXUt3y1epHGyekKq9QoC3yVubqKgC5zlYc9xOsCsfQ+Hmg6RuRt1Zn23/gw6
XCyyJMDTMDbRuJq1UsV0cJaeapsJ1omQlIET6xMZq0x7vBWYVK9USfc1HkoZeHcu
QEQtNAknEM4PDRRheV0/OAdb6PQYJX8TSviFHY+tustAidIODyFyr7EUfC2tffpP
aOdo/HgOPe+whjSNya2/ZF/jzTWo6UlRvaa/sttmYHnrAB4YQcBvsLsEsYzewrNm

=iJzl
-----END PGP PUBLIC KEY BLOCK-----
```