Viaa CSIRT profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version **1.0** of **23-04-2020** .

1.2. Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3 .
E-mail notification of updates are sent to:

- All **Viaa CSIRT** members
- All **Viaa CSIRT** constituents
- SURFcert (cert@surfnet.nl. , more information see https://www.trusted-introducer.org/teams/surfcert.html

  Any questions about updates please address to the **Viaa CSIRT** e-mail address.

1.3. Locations where this Document May Be Found

The current version of this profile is always available on **https://www.viaa.nl/security**

2. Contact Information

2.1. Name of the Team

Full name: **Viaa Hogeschool CSIRT**
Short name: **Viaa CSIRT**
Viaa CSIRT is the Computer Security Incident Response Teams team for the **Viaa Hogeschool** in The Netherlands**.**

2.2. Address

Viaa Hogeschool
Grasdorpstraat 2
8012 EN Zwolle
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST, according to EC rules)

2.4. Telephone Number

+31 (0)38 4255542

2.5. Facsimile Number
Viaa CSIRT can NOT be contacted by Facsimile.

2.6. Other Telecommunication
Not available.

2.7. Electronic Mail Addresses

csirt@Viaa.nl ; cert@Viaa.nl ; abuse@Viaa.nl ; security@Viaa.nl

These addresses can be used to report all security incidents to which relate to the **Viaa CSIRT** constituency, including copyright issues, spam and abuse.

2.8. Public Keys and Encryption Information
Encryption for secure communication is NOT supported .

2.9. Team Members
No information is provided about the **Viaa CSIRT** team members in public.

2.10. Other Information

- See the **Viaa CSIRT** webpages https://www.viaa.nl/security/

2.11. Points of Customer Contact
Regular cases: use **Viaa CSIRT** e-mail address.
Regular response hours: Monday-Friday, 09:00-16:00 (except public holidays in The Netherlands).
EMERGENCY cases: send e-mail with EMERGENCY in the subject line.

3. Charter

3.1. Mission Statement
The mission of **Viaa CSIRT** is to co-ordinate the resolution of IT security incidents related to their constituency (see 3.2), and to resolve IT security incidents, and help prevent such incidents from occurring.
All IT security incidents (including abuse) related to the domain Viaa.nl and gh.nl can be reported to **Viaa CSIRT**.

3.2. Constituency

The constituency for **Viaa CSIRT** is the Viaa Hogeschool in The Netherlands**.**
This constituency consists of:

- Employees and hired staff of the Viaa Hogeschool and its affiliate institutions. Students
- and guests of the university if and when they use a computer with an IP-address in the range that is controlled by the university.

The Viaa Hogeschool uses the IPv4 range 195.169.30.0 - 195.169.30.255

3.3. Sponsorship and/or Affiliation

Viaa CSIRT is part of Viaa Hogeschool.
https://www.viaa.nl/

3.4. Authority

The team coordinates security incidents on behalf of their constituency and has no authority reaching further than that. The team is however expected to make operational recommendations in the course of their work. Such recommendations can include but are not limited to blocking addresses or networks. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY. **Viaa CSIRT** itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to **Viaa CSIRT** as EMERGENCY, but it is up to **Viaa CSIRT** to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by **Viaa CSIRT**, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of

sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

Viaa CSIRT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/ISTLPv11.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

Viaa CSIRT will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymised fashion.

If you object to this default behavior of **Viaa CSIRT**, please make explicit what **Viaa CSIRT** can do with the information you provide. **Viaa CSIRT** will adhere to your policy, but will also point out to you if that means that **Viaa CSIRT** cannot act on the information provided.

Viaa CSIRT does not report incidents to law enforcement, unless national law requires so. Likewise, **Viaa CSIRT** only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that **Viaa CSIRT** cooperates in an investigation. When a court order is absent, **Viaa CSIRT** will only provide information on a need-to-know base.

4.3. Communication and Authentication

See 2.8 above.
No PGP/GnuPG is currently supported.
In all cases where highly sensitive information is involved, you are recommended to contact Viaa CSIRT by phone or in person on site. If needed, a method of communication will then be established which satisfies the security demands on both sides.

In cases where there is doubt about the authenticity of information or its source, **Viaa CSIRT** reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

Viaa CSIRT is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). **Viaa CSIRT** therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however **Viaa CSIRT** will offer support and advice on request.

5.2. Proactive Activities

Viaa CSIRT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.
Viaa CSIRT advises **Viaa Hogeschool** on matters of computer and network security. It can do so pro-actively in urgent cases, or on request.
Both roles are roles of consultancy: **Viaa CSIRT** is not responsible for implementation.

6. Incident reporting Forms

Not available. Preferably report in plain text using e-mail - or use the phone.

7. Disclaimers None.