CSIRT Viaa profile

Established according to RFC-2350.

1. Document Information

1.1. Date of Last Update

This is version **1.0** of **28-02-2025** .

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 **CSIRT Viaa** members
- All **CSIRT Viaa** constituents
- SURFcert (cert@surfcert.nl) , more information see
  https://www.trusted-introducer.org/teams/surfcert.html
  Any questions about updates please address to the **CSIRT Viaa** 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: **CSIRT Viaa Hogeschool**
Short name: **Viaa CSIRT**
CSIRT Viaa is the Computer Security Incident Response Teams team for the **Viaa Hogeschool** in The Netherlands**.**

2.2. Address

Viaa Hogeschool
Wethouder Alferinkweg 2
8012 GA 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 **CSIRT Viaa** team members in public.

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

2.11. Points of Customer Contact
Regular cases: use **CSIRT Viaa** 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 **CSIRT Viaa** 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 **CSIRT Viaa**.

3.2. Constituency

The constituency for **CSIRT Viaa** 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

CSIRT Viaa 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. **CSIRT Viaa** itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to **CSIRT Viaa** as EMERGENCY, but it is up to **CSIRT Viaa** 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 **CSIRT Viaa**, 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 TRAFFIC LIGHT PROTOCOL (TLP) - FIRST Standards Definitions and Usage Guidance) - information that comes in with the tags TLP:RED, TLP:AMBER, TLP:GREEN, and TLP:CLEAR will be handled appropriately.

CSIRT Viaa 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 anonymized fashion.

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

CSIRT Viaa does not report incidents to law enforcement, unless national law requires so. Likewise, **CSIRT Viaa** 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 **CSIRT Viaa** cooperates in an investigation. When a court order is absent, **CSIRT Viaa** will only provide information on a need-to-know base.

4.3. Communication and Authentication

See2.8 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, **CSIRT Viaa** reserves the right to authenticate this by any (legal) means.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

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

5.2. Proactive Activities

CSIRT Viaa pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.

CSIRT Viaa 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: **CSIRT Viaa** 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.