CSIRT Description for WWU-CERT

1. About this Document

This document contains a description of **WWU-CERT** according to RFC 2350. It provides information about WWU-CERT, how to contact the team, and describes its responsibilities and offered services.

1.1 Date of Last Update

This is version 1.2, published 2021/04/27.

1.2 Distribution List for Notifications

Notifications about updates to this document will be distributed via the internal mailing list iv-sicherheit@uni-muenster.de. External users should check the locations below for the latest version and use that one.

1.3 Locations Where this Document May Be Found

The current version of this CSIRT description document is available from the WWU-CERT website:

- **English:** https://www.uni-muenster.de/ziv.cert/CSIRT-descr-en.pdf
- **German:** https://www.uni-muenster.de/ziv.cert/CSIRT-descr-de.pdf

1.4 Authenticating this Document

Both versions of this document have been signed with WWU-CERT's PGP key. The key's fingerprint can be found in section 2.8 or on the WWU-CERT website. The public key can be downloaded from the usual key servers.
The individual signatures for each file can be found under:

- https://www.uni-muenster.de/ziv.cert/CSIRT-descr-en.pdf.asc
- https://www.uni-muenster.de/ziv.cert/CSIRT-descr-de.pdf.asc

2. Contact Information

2.1 Name of the Team

WWU-CERT: Computer Emergency Response Team of Westfälische Wilhelms-University (WWU) Münster

2.2 Address

WWU IT
WWU-CERT
Röntgenstr. 7-13
48149 Münster
Germany

2.3 Time Zone

Europe/Berlin, GMT+0100 (GMT+0200 from April to October)

2.4 Telephone Number

`+49 251 83 31600` (ask for WWU-CERT)

2.5 Facsimile Number

`+49 251 83 31552` (this is *not* a secure fax)

2.6 Other Telecommunication

Some members from WWU-CERT are active on various CSIRT online platforms, e.g. chat servers of Trusted Introducer (TI) or German CERT alliance CERT-Verbund.

2.7 Electronic Mail Address

- cert@uni-muenster.de - This is the primary address which should be used for incident reports.
- spam@uni-muenster.de - Special address for reporting phishing/spam messages related to the University of Münster (WWU).

2.8 Public Keys and Other Encryption Information

WWU-CERT has a PGP key, whose KeyID is 0xC01D356E with the following fingerpint:

- `DAFE C355 08F3 CB67 2DF7 C3C2 76E4 1181 C01D 356E`

The public key and its signatures can be found on common public keyservers, e.g. https://pgp.surfnet.nl.

WWU-CERT also has a X.509 key, whose KeyID currently is 0x225CEDC99156B5C37FF43DCB with the following fingerprint:

- `7F89 6686 0475 8F21 5883 885A 1B4B A1C8 60B4 AA62`

The public key can be found on the DFN-PKI keyserver.

2.9 Team Members

Thorsten Küfer (WWU IT), CISO at University of Münster (WWU), (PGP KeyID: 0x4CD0C117) is the current WWU-CERT coordinator. For easier updating and to keep this document short, backup coordinators and other team members are listed on the WWU-CERT website.

Management, liaison and supervision are provided by Dr. Raimund Vogl, CIO at University of Münster (WWU) and Director of the university's IT center (WWU IT).

2.10 Other Information

Since 2018 WWU-CERT is a member of the German CERT alliance CERT-Verbund and EDUCV, a national group of CSIRTs from higher education institutions in Germany. Furthermore WWU-CERT is a listed team at the Trusted Introducer (TI) Service since 2018/08/28.

More information can be found on the WWU-CERT website.

2.11 Points of Customer Contact

The preferred method for contacting WWU-CERT is via e-mail at cert@uni-muenster.de. Messages sent to this address will be forwarded to the team's ticketing system and will be reviewed by the team members on duty.

If it is not possible (or not advisable for security reasons) to use e-mail, WWU-CERT can be reached by telephone during regular office hours. Telephone messages are checked less often than e-mail.

WWU-CERT's hours of operation are generally restricted to regular business hours (07:00-17:00, Monday to Friday except holidays) and messages outside of those times will be answered on the next business day. In the event of an urgent emergency situation involving WWU-CERT's constituency outside the usual business hours, the Network Operating Center (NOC) on-call staff can be alerted.

3. Charter

3.1 Mission Statement

The purpose of WWU-CERT is to assist the University of Münster (WWU) community in responding to IT security incidents when they occur and to assist members of the constituency in implementing proactive measures to reduce the risk of such incidents (for example by finding security issues). The main goal is to protect the University of Münster (WWU), including its community and infrastructure, from negligent or illegal usage of its IP addresses or resources. WWU-CERT acts as the central coordinator for IT security related events and information in its constituency.

3.2 Constituency

WWU-CERT's constituency is defined as the community of the University of Münster (WWU), including but not limited to employees, students and general users of the university's IT systems (see "Policy on Information Security" (ISL-WWU)). This also includes decentralized departments of the university and their members. WWU-CERT is responsible for investigating IT security incidents related to all on-site systems of the university, as well as devices connecting to the university's networks. The support given varies depending on the system's location and type, as well as the related users' groups.

WWU-CERT provides services for the following public IP address spaces:

- 128.176.0.0/16
- 185.151.152.0/22
- 193.175.4.0/24
- 212.201.144.0/21
- 2001:638:500::/48
- 2001:4cf0::/29

As well as for the following domains:

- uni-muenster.de
- wwu.de
- wwu.io

3.3 Sponsorship and Affiliation

WWU-CERT was established on the 2000/01/14 and is sponsored by the IT center (WWU IT) of University of Münster (WWU). It is part of the executive department for IT security and cooperates closely with the IT security team (see ISL-WWU). Its offices have been established at the IT center.

WWU-CERT maintains affiliations with DFN-CERT and various university CSIRTs throughout Germany on an as-needed basis. The team is active in the CERT-Verbund, EDUCV and TF-CSIRT communities.

3.4 Authority

WWU-CERT operates under the patronage of, and with authority delegated by, the IT center (WWU IT) of University of Münster (WWU). This was defined and passed in the university's "Policy on Information Security" (see ISL-WWU).

WWU-CERT expects to work cooperatively with system administrators and users from the constituency, and, as far as possible, to avoid authoritarian relationships. However, should circumstances warrant it, WWU-CERT will appeal to the IT center (WWU IT) to exert its authority, direct or indirect, as necessary, e.g. through deactivation of user accounts or blocking of network access for devices.

Members of the constituency who wish to appeal the actions of WWU-CERT should contact the Chief Information Officer (CIO) or the IT commission of University of Münster (WWU).

4. Policies

4.1 Types of Incidents and Level of Support

WWU-CERT is authorized to address all types of IT security incidents or issue which occur, or threaten to occur, related to the University of Münster (WWU).

The level of support given by WWU-CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, the affected systems and WWU-CERT's available resources at the time. Resources will be assigned according to the following priorities, listed in decreasing order:

- Threats to the physical safety of human beings.
- Root or system-level attacks on any central IT-management system or any part of the backbone network infrastructure.
- Root or system-level attacks on any large public service machine, either multi-user or dedicated-purpose.
- Compromise of restricted confidential service accounts or software installations, e.g. accounts or systems used for central administration.
- Denial of service attacks on any of the above three items.
- Any of the above, originating from University of Münster (WWU) and concerning foreign systems.
- Large-scale attacks of any kind, e.g. sniffing attacks, social engineering attacks, password cracking attacks.
- Threats, harassment, and other criminal offenses involving individual user accounts.
- Compromise of individual user accounts on multi-user systems.
- Compromise of desktop systems.
- Forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. copyright infringements or e-mail forgery.
- Denial of service on individual user accounts, e.g. mailbombing.

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent. Classification of incidents is loosely adapted from Trusted Introducer (TI) Incident Classification.

In general no direct support will be given to end users. They are expected to contact the responsible system administrator or IT security officer (IV-SB) of their IT support unit (IVV), the IT user support or their department head for assistance. WWU-CERT will support the latter group of people.

While WWU-CERT understands that there exists great variation in the level of system administrator expertise, and while the team will endeavor to present information and assistance at a level appropriate to each person, WWU-CERT cannot train system administrators on the fly, and it cannot perform system maintenance on their behalf. In most cases WWU-CERT will provide pointers to the information needed to implement appropriate measures. System administrators should contact the IT security officer (IV-SB) of their department for further support.

WWU-CERT is committed to keeping the IT security officers (IV-SB) and the group of system administrators informed about potential vulnerabilities, and where possible, will inform this community via the internal mailing list iv-sicherheit@uni-muenster.de of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

All information handled by WWU-CERT is treated as confidential by default and will only be shared on an as-needed basis. Team members signed a non-disclosure agreement (NDA) and agreed to comply with common sharing policies, e.g. the Traffic Light Protocol (TLP). WWU-CERT strives to comply with the Trusted Introducer (TI) CSIRT Code of Practice (CCoP).

Because of the nature of their responsibilities and consequent expectations of confidentiality, management members of University of Münster (WWU) and the IT center (WWU IT) are entitled to receive whatever information is necessary to facilitate the handling of IT security incidents which occur in their jurisdictions. IT security officers (IV-SB) and system administrators at University of Münster (WWU) are, by virtue of their responsibilities, trusted with confidential information. However, unless such people are also members of WWU-CERT, they will be given only that confidential information which they must have in order to assist with an investigation, or in order to secure their own systems. Users of services offered by the University of Münster (WWU) are entitled to information regarding the safety of their own user accounts and will be notified if their account is believed to have been compromised.

Since WWU-CERT wants to support the IT security community, it encourages and supports the sharing of incident related information, e.g. IOAs/IOCs, with other trusted teams or institutions. If specific information is deemed useful to prevent or solve incidents at other institutions, it will be shared freely. In order to respect ethical and legal restrictions, measures to anonymize personally identifiable information (PII) and other sensitive details will be used as far as possible.

WWU-CERT co-operates with law enforcement entities, in accordance with the IT usage policy for the university (see here), and sharing of confidential information may be needed or even legally required in certain cases to pursue an investigation. Those cases will usually be handled through the university's legal department. The amount of shared information will always be restricted to the necessary minimum.

Confidential information will not be disclosed to the whole constituency or even the general public. Should the release of information at a large scale be necessary, it will be handled through the university's legal or public relations departments.

4.3 Communication and Authentication

In view of the types of information that WWU-CERT will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP or S/MIME end-to-end encryption will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be end-to-end encrypted for transmission. To verify the source and the integrity of transmitted data, digital signatures will be used where possible. For this purpose all e-

mails containing official statements on behalf of the team or team members will be signed using PGP or S/MIME signatures.

WWU-CERT supports the use of the Traffic Light Protocol (TLP) and will respect sharing restrictions.

Where it is necessary to establish trust, for example before relying on information given to WWU-CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within University of Münster (WWU), and with known CERTs or CSIRTs, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, along with telephone call-back or signed e-mail mail-back to ensure that the party is not an impostor. Incoming e-mails whose data must be trusted will be checked with the originator personally or by means of digital signatures (PGP or S/MIME are supported).

4.4 Reaction Time

Usually the first response happens timely at the same working day, if not, a team member will respond within two business days.

5. Services

WWU-CERT offers several services from different areas related to IT security. Most services will only be offered to members of the constituency and their devices, while others might be available for external parties as well. Available services are categorized according to FIRST's CSIRT Services Framework v2.1 and will be listed in a brief fashion to keep this document short. Descriptions of the service areas and each individual service can be found in the framework. Further details about some of the services can also be found on the team's website.

5.1 Information Security Event Management

- Monitoring and Detection
- Event Analysis

5.2 Information Security Incident Management

- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis

  (Only in special cases and within a limited scope)
- Mitigation and Recovery

  (Limited to coordination and providing support for affected parties)
- Information Security Incident Coordination
- Crisis Management Support

5.3 Vulnerability Management

- Vulnerability Report Intake
- Vulnerability Analysis

  (Limited scope to be able to support remediation)

- Vulnerability Disclosure
- Vulnerability Response

  (Limited to detection/scanning tasks and supporting remediation)

5.4 Situational Awareness

- Data Acquisition
- Analysis and Synthesis
- Communication

5.5 Knowledge Transfer

- Awareness Building

  (Only in a supporting role for the IT security team)
- Training and Education

  (Only offered in a limited scope)
- Technical and Policy Advisory

  (Only in a supporting role for the IT security team)

6. Incident Reporting Forms

There are no special forms for reporting incidents to WWU-CERT available yet, but incident reports should contain the following information, to ensure fast investigation and remediation:

- Incident date and time (including time zone)
- Source IPs, ports and protocols (where applicable)
- Destination IPs, ports and protocols (where applicable)
- Incident description and further details

Preferable the report should also include related log files in a common format, e.g. Syslog or Common Event Format (CEF). When forwarding suspicious e-mail messages please make sure to forward them as attachments so that all e-mail headers are included.

In case of reporting discovered vulnerabilities we ask that common responsible disclosure guidelines will be followed, e.g. no abuse of said vulnerability, end-to-end encryption when transmitting sensitive data and no disclosure of the vulnerability to other parties until the problem is resolved.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, WWU-CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within. That includes this document, which is provided 'as is' without warranty of any kind, either expressed or implied.

If you notice any mistakes within this document please send a message to WWU-CERT via e-mail. We will try to resolve such issues in the next version.

8. Copyright