12/12/2025

MENNEKES

RI

G-RI-030

Version: 1.0

not restricted

Guideline MENNEKES Group

Coordinated Vulnerability Disclosure

Creator: Patrick Pfau

Approver: Jürgen Bechtel

I Scope

MENNEKES group

II Purpose

This policy explains how MENNEKES deals with responsible disclosures / coordinated vulnerability disclosures of technical software vulnerabilities.

III Implementation & observance

Central Information Security / Product Security

IV Consequences of non-compliance or non-observance

- Different and wrong handlings of vulnerabilities
- Too early disclosure of vulnerabilities without having them fixed
- False or missing communication
- Information security incidents
- Law violations

1 Introduction

MENNEKES is committed to ensuring the security of customers, employees, the public and all other stakeholders by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to us.

This policy describes **what systems and types of research** are covered under this policy, **how to send us vulnerability reports**, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities. We encourage you to contact us to report potential vulnerabilities in our systems and products.

2 Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized we will work with you to understand and resolve the issue quickly, and MENNEKES will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

3 Code of Conduct

Under this policy, “research” means activities in which you:

- notify us as soon as possible after discovering an actual or potential security issue in a product/system where MENNEKES acts as the manufacturer (product) or as the operator (internal IT systems).
- make every effort to avoid privacy breaches, impairments of user experience, disruptions of production systems, as well as destruction or manipulation of data.
- do not abuse exploits and only use them to the extent necessary to confirm the existence of a vulnerability. Do not use an exploit to compromise or exfiltrate data, establish persistent command-line access, or leverage the exploit to access other systems.
- have not abused the reported vulnerability. This means no damage beyond the reported vulnerability has been caused.
- have not offered tools or code for exploiting vulnerabilities - e.g., on darknet markets, for a fee or free of charge - that third parties could use to commit crimes.
- give us a reasonable amount of time to fix the issue (see Timeline) before publicly disclosing the vulnerability.
- do not submit a large number of low-quality reports.
- ensure your vulnerability report relates to publicly unknown information and is not the result of automated tools or scans without supporting documentation. Information about already fixed vulnerabilities will still be received and reviewed, even if such reports do not qualify for further processing under a Responsible Disclosure process.

Once you determine that a vulnerability exists or encounter sensitive data (including personal data, financial information, protected information, or trade secrets of any party), **you must stop your testing, notify us immediately, and not disclose this data to anyone else**. Failure to comply with these requirements means we will handle your report as best as possible, but you will lose any eligibility to participate in the Bug Bounty Program or be listed on our Hall of Fame webpage.

4 Test methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

5 Scope

This policy applies to all products and systems produced or operated by MENNEKES. Furthermore, vulnerabilities found in systems or products of our vendors/service providers/suppliers are not covered by this policy and should be reported directly to the vendor in accordance with their disclosure policy (if available). If you are unsure whether a product or system falls within the scope, please contact us before starting your research.

We ask that active research and testing be conducted only on systems and products that fall within the scope of this policy. If there is a specific system that is out of scope but you believe should be tested, please contact us first to discuss this.

This policy is effective immediately upon publication in its current version for all ongoing and future reporting procedures.

6 Reporting a vulnerability

6.1 Purpose and contact

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely MENNEKES, we may share your report in accordance with applicable laws.

We accept vulnerability reports at this form or via psirt@mennekes.org **(product vulnerabilities) or** csirt@mennekes.org **(infrastructure vulnerabilities)**. We do support and recommend encrypted and signed file transfer, such as PGP-encrypted emails, see more information at https://mennekes.org/.well-known/security.txt. The expiry date of the contact options is also written in the link. On request, you can also be sent a link to a secure data storage.

If you share contact information, we will acknowledge receipt of your report.

By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against MENNEKES related to your submission. MENNEKES will review the reported vulnerability as part of the “Bug Bounty” program (see chapter Bug Bounty) and, if positively evaluated and in compliance with the requirements, offer you a reward.

6.2 Report anonymously

Reports may be submitted anonymously. If you wish to do so, please use the form from our website. Please be aware, that further explanations and documentation may be required, particularly for complex problems that cannot be addressed in anonymous submission. Your submitted vulnerability report may then only be processed to a limited extent or may not be processed at all. Nevertheless MENNEKES will treat anonymous reports in the best possible way.

6.3 What we would like to see from you

In addition to complying with the topics mentioned under the Code of Conduct, we recommend, to support prioritization and processing of submissions, that your reports include as much information as possible, including:

- your contact data (at least email address (preferred) or telephone number),
- description of the location and exact product with version number or system where the vulnerability was discovered,
- the potential impact of exploitation (if possible),
- a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful),
- English or german language.

6.4 What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

6.4.1 Timeline

In general you are welcome to ask for the current status of your submission, but we will come back to you proactively according to the following timeline:

- Within 5 business days, we will acknowledge that your report has been received.
- Within 10 business days, we will confirm or deny the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution.
- Within 90 business days after confirming the existence of a product vulnerability, we will publicly disclose validated and verified reported vulnerabilities and – where possible – provide a version with the vulnerability fixed. If there is a valid justification and explanation for a delay in remediation or fixing the vulnerability, the period for public disclosure and providing the fix may be extended once by an additional 90 days. In exceptional cases, and in coordination with the responsible CSIRT, the period for public disclosure may be further extended upon request by MENNEKES.

6.4.2 Bug Bounty

The reported vulnerability will be reviewed and assessed by MENNEKES Information Security. The assessment is based on the “Common Vulnerability Scoring System” (CVSS) Calculator (Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) in combination with the individual classification of the affected systems and/or data.

The determined risk potential, consisting of the CVSS score and individual evaluation, is linked to a reward system (Bug Bounty). The exact amount will be determined by the Information Security Officer of the MENNEKES Group.

Risk Potential	Low	Medium	High	Critical
Bug Bounty (Net amount before value-added tax)	none	100 – 500 Euro	501 – 1.000 Euro	1.001 - 5.000 Euro

Special Rules for the Bug Bounty Program:

- Only the initial report of a vulnerability that is not yet known to MENNEKES is eligible for a Bug Bounty payout.
- The program is public; anyone can participate. Excluded from the reward program are current and former employees of the MENNEKES Group and affiliated companies, their relatives or legal representatives, as well as service providers and suppliers.
- Only vulnerabilities in not end-of-life products, systems, or components that MENNEKES develops and can directly influence are eligible for a Bug Bounty payout. Excluded are third-party software that is only integrated, as well as closed-source components from suppliers.
- MENNEKES Information Security determines the payout amount. A payout can only be made if the participant in the Bug Bounty Program issues an invoice to the MENNEKES Group that complies with applicable VAT regulations.
- Payments are made exclusively by bank transfer. Payments via PayPal, cryptocurrencies, etc., are excluded.
- MENNEKES is particularly interested in vulnerabilities that allow unauthorized access to confidential data, modification or deletion of such data. Vulnerabilities affecting products that allow unauthorized parties to negatively impact confidentiality, integrity, or availability are also of special interest.
    - Examples of relevant vulnerabilities can be found at OWASP (https://owasp.org/www-project-top-ten/), such as:
        - Cross-site request forgery (CSRF / XSRF) (https://de.wikipedia.org/wiki/Cross-Site-Request-Forgery)
        - Persistent Cross-Site Scripting (XSS) (https://www.enisa.europa.eu/topics/incident-response/glossary/cross-site-scripting-xss)
        - SQL Injections (https://owasp.org/www-community/attacks/SQL_Injection)
        - Remote Code Executions
    - Not relevant and therefore excluded from the Bug Bounty Program include, for example:
        - Basic reachability of digital services
        - Actions involving direct physical access to systems or devices

- Phishing emails, especially those misusing MENNEKES Group email addresses
- Vulnerabilities without proof of exploitability
- Vulnerabilities affecting only outdated browsers or those operated with limited security features
- Attacks that require a victim to intentionally or unintentionally share or disclose a privileged (access) token (e.g., Personal Access Token, OAuth token, project or group access token, deploy token, session token, or runner authentication token). Reports about leaked access tokens from employees of the MENNEKES Group remain in scope and are eligible for bug bounty rewards.
- Reports generated by scanners or automated tools without clear and fully verifiable reference to a vulnerability
- Missing best practices in headers, SSL/TLS, DNS
- Missing headers without direct negative impact
- Clickjacking
- Banner/versions, directory listing of static assets, stack traces on non-sensitive paths, comments in JS
- Weak TLS algorithms and outdated TLS versions
- Missing or incorrect SPF entries of any kind
- Missing or incorrect DMARC entries of any kind
- Vulnerabilities related to source code disclosure
- Disclosure of non-confidential information
- Email bombing
- Request flooding & DoS/DDoS
- Missing rate limiting
- CSV injection

6.4.3 In general

- we maintain an open dialogue to discuss issues without requiring an NDA to be signed.
- we do not share any personal data such as your name or contact details with third parties without your explicit consent.
- we ensure that the conversation remains confidential within the framework of legal requirements.
- we make sure to be a trusted point of contact throughout the entire process for a reliable and respectful exchange.
- upon request, we will publish your name/alias and a desired reference on our recognition website (Hall of Fame) after a valid vulnerability has been reported and the disclosure process has been completed. All parties involved treat each other with respect, and there is no room for unlawful behaviour such as discrimination, sexism, racism, Nazism, glorification of violence, pornography, insults, defamation, or slander. In the event of a violation in this regard, MENNEKES will refrain from publication.
- we ensure that product vulnerabilities are publicly disclosed in coordination with the responsible CSIRT.

7 End of process

MENNEKES will end the coordinated vulnerability / responsible disclosure process and inform the researcher (if not submitted anonymously) without undue delay,

- if the findings of the vulnerability are unfounded,
- when the vulnerability of a product, system or service has been fixed and made public,
- if the vulnerability has been fixed or mitigated by an appropriate patch and made publicly available,
- if the vulnerability has been made public and, in consultation with the responsible CSIRT, it can no longer be assumed that the vulnerability will be mitigated or remedied.

8 Questions

Questions regarding this policy or to the status of any reported vulnerability are welcome. They can be sent to psirt@mennekes.org or csirt@mennekes.org. We also invite you to contact us with suggestions for improving this policy.