12.12.2025

MENNEKES

RI

G-RI-030

Version: 1.0

nicht eingeschränkt

Unternehmensrichtlinie MENNEKES Gruppe

Koordinierte Offenlegung von Schwachstellen

Ersteller: Patrick Pfau

Freigeber: Jürgen Bechtel

I Geltungsbereich

MENNEKES group

II Zweck

Diese Richtlinie erläutert, wie MENNEKES mit verantwortungsvollen Offenlegungen/koordinierten Offenlegungen von technischen (Software-)Schwachstellen umgeht.

III Umsetzung & Einhaltung

Zentrale Informationssicherheit / Produktsicherheit

IV Folgen bei Nichteinhaltung oder Nichtbeachtung

- Unterschiedlicher und falscher Umgang mit Schwachstellen
- Zu frühe Bekanntgabe von Schwachstellen, ohne diese geschlossen zu haben
- Falsche oder fehlende Kommunikation
- Informationssicherheitsvorfälle
- Gesetzesverstöße

1 Einleitung

MENNEKES verpflichtet sich, die Sicherheit von Kunden, Mitarbeitern, der Öffentlichkeit und allen anderen Interessengruppen zu gewährleisten, indem ihre Informationen geschützt werden. Diese Richtlinie soll Sicherheitsforschern klare Richtlinien für die Durchführung von Schwachstellenentdeckungsaktivitäten geben und unsere Präferenzen für die Einreichung entdeckter Schwachstellen an uns vermitteln.

Diese Richtlinie beschreibt, **welche Systeme und Arten von Forschung** unter diese Richtlinie fallen, **wie Sie uns Schwachstellenberichte senden** können und **wie lange** wir Sicherheitsforscher bitten, mit der öffentlichen Offenlegung von Schwachstellen zu warten. Wir ermutigen Sie, uns zu kontaktieren, um potenzielle Schwachstellen in unseren Systemen und Produkten zu melden.

2 Autorisierung

Wenn Sie sich bei Ihrer Sicherheitsforschung in gutem Glauben bemühen, diese Richtlinie einzuhalten, werden wir Ihre Forschung als autorisiert betrachten. Wir werden mit Ihnen zusammenarbeiten und um das Problem schnell zu verstehen und zu lösen, wird MENNEKES keine rechtlichen Schritte im Zusammenhang mit Ihrer Forschung empfehlen oder einleiten. Sollte ein Dritter rechtliche Schritte gegen Sie einleiten, weil Sie Aktivitäten durchgeführt haben, die im Einklang mit dieser Richtlinie stehen, werden wir diese Autorisierung bekannt machen.

3 Verhaltenskodex

Unter dieser Richtlinie bedeutet „Forschung“ solche Aktivitäten, bei denen Sie

- uns so schnell wie möglich benachrichtigen, nachdem Sie ein tatsächliches oder potenzielles Sicherheitsproblem eines Produkts/Systems entdeckt haben, bei dem MENNEKES als Hersteller (Produkt) oder als Betreiber (der internen IT-Systeme) agiert.
- alle Anstrengungen unternehmen, um Datenschutzverletzungen, Beeinträchtigungen der Benutzererfahrung, Störungen von Produktionssystemen sowie Zerstörung oder Manipulation von Daten zu vermeiden.
- Exploits nicht missbrauchen und nur in dem Maße verwenden, wie es notwendig ist, um das Vorhandensein einer Schwachstelle zu bestätigen. Verwenden Sie keinen Exploit, um Daten zu kompromittieren oder zu exfiltrieren, dauerhaften Zugriff auf die Befehlszeile zu etablieren oder den Exploit zu nutzen, um auf andere Systeme zuzugreifen.
- die gemeldete Schwachstelle nicht missbraucht haben. Das bedeutet, dass kein Schaden über die gemeldete Schwachstelle hinaus verursacht wurde.
- keine Werkzeuge und keinen Code zur Schwachstellenausnutzung, z.B. auf Darknet-Märkten, gegen Gebühr oder kostenlos angeboten haben, die Dritte zur Begehung von Straftaten nutzen könnten.
- uns eine angemessene Zeit zur Behebung des Problems geben (siehe Zeitplan), bevor die Schwachstelle öffentlich bekannt gemacht wird.
- keine große Menge an Berichten niedriger Qualität einreichen.
- sicherstellen, dass sich Ihr Schwachstellenbericht auf öffentlich unbekannte Informationen bezieht und die Schwachstellenberichte nicht das Ergebnis automatisierter Tools oder Scans ohne unterstützende Dokumentation sind. Informationen über bereits behobene Schwachstellen werden dennoch empfangen und überprüft, auch wenn dieser Bericht nicht für eine weitere Bearbeitung im Rahmen eines Responsible Disclosure-Prozesses qualifiziert ist.

Sobald Sie festgestellt haben, dass eine Schwachstelle existiert oder auf sensible Daten stoßen (einschließlich personenbezogener Daten, Finanzinformationen oder geschützter Informationen oder Geschäftsgeheimnisse einer Partei), **müssen Sie Ihren Test stoppen, uns sofort benachrichtigen und diese Daten niemandem sonst offenlegen**. Bei Nichteinhaltung der Vorgaben werden wir Ihren Bericht zwar bestmöglich behandeln, es entfallen jedoch jegliche Möglichkeiten auf die Teilnahme am Bug Bounty Programm und der Nennung auf unserer Hall of Fame-Webseite.

4 Testmethoden

Die folgenden Testmethoden sind nicht autorisiert:

- Netzwerk-DoS- oder DDoS-Tests oder andere Tests, die den Zugriff auf ein System oder Daten beeinträchtigen oder beschädigen.
- Physische Tests (z.B. Zugang zu Büros, offene Türen), Social Engineering (z.B. Phishing, Vishing) oder andere nicht-technische Schwachstellentests.

5 Anwendbarkeit

Diese Richtlinie gilt für alle Produkte und Systeme, die von MENNEKES produziert oder betrieben werden. Darüber hinaus fallen Schwachstellen, die in Systemen oder Produkten unserer Anbieter/Dienstleister/Lieferanten gefunden werden, nicht in den Geltungsbereich dieser Richtlinie und sollten direkt dem Anbieter gemäß seiner Offenlegungsrichtlinie (falls vorhanden) gemeldet werden. Wenn Sie sich nicht sicher sind, ob ein Produkt oder System im Geltungsbereich liegt oder nicht, kontaktieren Sie uns bitte, bevor Sie mit Ihrer Forschung beginnen.

Wir bitten darum, dass aktive Forschung und Tests nur an den Systemen und Produkten durchgeführt werden, die unter den Geltungsbereich dieser Richtlinie fallen. Wenn es ein bestimmtes System gibt, das nicht im Geltungsbereich liegt, das Ihrer Meinung nach jedoch getestet werden sollte, kontaktieren Sie uns bitte zuerst, um dies zu besprechen.

Diese Richtlinie ist unmittelbar nach Veröffentlichung in der jeweils aktuellen Fassung für alle laufenden und künftigen Meldeverfahren gültig.

6 Melden von Schwachstellen

6.1 Zweck und Kontakt

Informationen, die im Rahmen dieser Richtlinie eingereicht werden, werden ausschließlich zu Mitigationsmaßnahmen verwendet – zur Minderung oder Behebung von Schwachstellen. Wenn Ihre Erkenntnisse neu entdeckte Schwachstellen umfassen, die alle Benutzer eines Produkts oder Dienstes betreffen und nicht nur MENNEKES, können wir Ihren Bericht gemäß den geltenden Gesetzen weitergeben.

Wir akzeptieren Schwachstellenberichte über dieses Formular oder per E-Mail an psirt@mennekes.org (Produkt-Schwachstellen) oder csirt@mennekes.org (Infrastruktur-Schwachstellen). Wir unterstützen und empfehlen verschlüsselte und signierte Dateiübertragungen, wie z.B. PGP-verschlüsselte E-Mails. Weitere Informationen wie bspw. die Downloadlinks oder Fingerprints finden Sie unter https://mennekes.org/.well-known/security.txt. Das Ablaufdatum der Kontaktoptionen wird ebenfalls in vorgenanntem Link bereitgestellt. Auf Anfrage können Sie auch einen Link zu einem sicheren Datenspeicher erhalten.

Wenn Sie Ihre Kontaktinformationen angeben, bestätigen wir den Erhalt Ihres Berichts.

Durch die Einreichung einer Schwachstelle erkennen Sie an, dass Sie keine Zahlung erwarten und ausdrücklich auf zukünftige Zahlungsansprüche gegen MENNEKES im Zusammenhang mit Ihrer Einreichung verzichten. MENNEKES wird die gemeldete Schwachstelle im Rahmen des „Bug Bounty“ Programms prüfen (siehe Kapitel Belohnung) und Ihnen bei positiver Bewertung und unter Beachtung der Vorgaben eine Prämie anbieten.

6.2 Anonym berichten

Berichte können anonym eingereicht werden. Wenn Sie dies wünschen, verwenden Sie bitte das Formular auf unserer Website. Bitte beachten Sie, dass für komplexe Probleme, möglicherweise weitere Erklärungen und Dokumentationen sowie Rückfragen an Sie erforderlich sind. Ihr eingereichter Schwachstellenbericht kann dann nur eingeschränkt oder gar nicht bearbeitet werden, daher empfehlen wir anonyme Berichte nicht, auch wenn MENNEKES anonyme Berichte bestmöglich behandeln wird.

6.3 Was wir von Ihnen erwarten

Neben der Einhaltung der unter Verhaltenskodex genannten Themen, empfehlen wir zur Unterstützung bei der Priorisierung und Bearbeitung von Einreichungen, dass Ihre Berichte so viele Informationen wie möglich enthalten, einschließlich:

- Ihrer Kontaktdaten (mindestens E-Mail-Adresse (bevorzugt) oder Telefonnummer),
- Beschreibung sowie Nennung des genauen Produkts inkl. Versionsnummer oder Systems, in dem die Schwachstelle entdeckt wurde,
- des potenziellen Ausnutzungsrisikos (falls möglich),
- einer detaillierten Beschreibung der Schritte, die erforderlich sind, um die Schwachstelle zu reproduzieren (Proof-of-Concept-Skripte oder Screenshots sind hilfreich),
- in englischer oder deutscher Sprache.

6.4 Was Sie von uns erwarten können

Wenn Sie sich entscheiden, Ihre Kontaktdaten mit uns zu teilen, verpflichten wir uns, so offen und schnell wie möglich mit Ihnen zu kommunizieren.

6.4.1 Zeitplan

Grundsätzlich sind Anfragen zum Status des Bearbeitungsstandes willkommen, wir werden jedoch proaktiv auf Sie innerhalb des folgenden Zeitplanes zukommen:

- Innerhalb von 5 Arbeitstagen bestätigen wir den Erhalt Ihres Berichts.
- Innerhalb von 10 Arbeitstagen bestätigen oder dementieren wir das Vorhandensein der Schwachstelle und sind so transparent wie möglich bei den Schritten, die wir während des Behebungsprozesses unternehmen, einschließlich etwaiger Probleme oder Herausforderungen, die die Lösung verzögern könnten.
- Innerhalb von 90 Arbeitstagen nach Bestätigung des Vorhandenseins einer Produkt-Schwachstelle werden wir validierte und verifizierte gemeldete Schwachstellen öffentlich bekannt machen und – sofern möglich – eine Version der behobenen Schwachstelle bereitstellen. Wenn es eine gültige Begründung und Erklärung für eine Verzögerung bei der Behebung oder Behebung der Schwachstelle gibt, kann der Zeitraum bis zur öffentlichen Bekanntmachung und der Bereitstellung der Fehlerbehebung einmalig um zusätzliche 90 Tage verlängert werden. In Ausnahmefällen und in Abstimmung mit dem zuständigen CSIRT kann der Zeitraum bis zur öffentlichen Bekanntmachung auf Antrag von MENNEKES weiter verlängert werden.

6.4.2 Belohnung

Die gemeldete Schwachstelle wird von der MENNEKES-Informationssicherheit geprüft und bewertet. Bewertungsgrundlage ist der „Common Vulnerability Scoring System“ (CVSS) Calculator (Link: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator) in Verbindung mit der individuellen Klassifizierung der betroffenen Systeme bzw. Daten.

An das ermittelte Gefahrenpotenzial bestehend aus CVSS-Score und individueller Bewertung ist ein Belohnungssystem (Bug Bounty) gekoppelt. Die genaue Höhe wird vom Informationssicherheitsbeauftragten der MENNEKES Gruppe festgelegt.

Gefahrenpotenzial	Niedrig	Mittel	Hoch	Kritisch
Bug Bounty (Nettobetrag vor Umsatzversteuerung)	kein	100 – 500 Euro	501 – 1.000 Euro	1.001 - 5.000 Euro

Besondere Regelungen zum Bug Bounty-Programm:

- Nur die erstmalige Meldung einer für MENNEKES noch nicht bekannten Schwachstelle kommt für eine Bug Bounty-Auszahlung in Frage
- Das Programm ist öffentlich, es kann jede*r teilnehmen. Ausgeschlossen vom Belohnungsprogramm sind lediglich aktuelle und ehemalige Mitarbeiterinnen und Mitarbeiter der MENNEKES Gruppe und der verbundenen Unternehmen, deren Angehörige oder ihre gesetzlichen Vertreter sowie Dienstleister und Lieferanten.
- Für eine Bug Bounty-Auszahlung kommen nur Schwachstellen von nicht End-of-Life-Produkten, Systemen oder Komponenten in Frage, die MENNEKES entwickelt und unmittelbar beeinflussen kann. Ausgeschlossen sind Drittanbieter-Software, die ausschließlich integriert wird sowie Closed-Source Komponenten von Zulieferern.
- Die Informationssicherheit von MENNEKES legt den Auszahlungsbetrag fest. Eine Auszahlung kann nur erfolgen, wenn der Teilnehmer am Bug Bounty Programm der

MENNEKES-Gruppe eine entsprechende und der geltenden Umsatzbesteuerung gerecht werdende Rechnung stellt.

- Auszahlungen erfolgen grundsätzlich nur per Banküberweisung. Zahlungen per PayPal, Crypto Währungen etc. sind ausgeschlossen.
- Hierbei sind für die MENNEKES Gruppe insbesondere Schwachstellen interessant, die es Unberechtigten ermöglichen auf vertrauliche Daten zuzugreifen, diese zu ändern oder zu löschen. Auch sind solche Schwachstellen besonders interessant, es Unberechtigten ermöglichen, die Vertraulichkeit, Integrität oder Verfügbarkeit negativ zu beeinflussen.
    - Beispiele für relevante Schwachstellen finden sich z. B. bei OWASP (https://owasp.org/www-project-top-ten/) wie z. B.
        - 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

    - Nicht relevant und damit ausgeschlossen für das Bug Bounty-Programm sind beispielweise:
        - Grundsätzliche Erreichbarkeit von digitalen Services
        - Aktionen bei direktem physischem Zugang auf Systeme oder Geräte
        - Phishing-Mails u. ä., insbesondere solche, in denen z. B. die Mailadressen der MENNEKES Gruppe missbraucht werden
        - Schwachstellen ohne Nachweis einer Ausnutzbarkeit
        - Schwachstellen, die nur veraltete oder mit eingeschränkten Sicherheitsmerkmalen betriebene Browser betreffen
        - Angriffe, die erfordern, dass ein Opfer einen privilegierten (Zugriffs-)Token absichtlich oder unabsichtlich weiter- oder preisgibt (z.B. Personal Access Token, OAuth-Token, Projekt- oder Gruppen-Access-Token, Deploy-Token, Session-Token oder Runner-Authentifizierungstoken. Meldungen über geleakte Zugriffstoken von Mitarbeitenden der MENNEKES Gruppe sind weiterhin im Geltungsbereich und Bug-Bounty berechtigt.
        - Von Scannern bzw. automatisiert erzeugte Berichte, die keinen konkreten und komplett nachvollziehbaren Bezug zu einer Schwachstelle ermöglichen
        - Nicht eingesetzte Best-Practices in Headern, SSL/TLS, DNS
        - Fehlende Header ohne direkte negative Auswirkungen
        - Clickjacking
        - Banner/Versionen, Directory Listing rein statischer Assets, Stacktraces auf nicht-sensiblen Pfaden, Kommentartexte in JS
        - Schwache TLS-Algorithmen und veraltete TLS-Versionen
        - Fehlende oder falsche SPF-Einträge jeglicher Art
        - Fehlende oder falsche DMARC-Einträge jeglicher Art
        - Schwachstellen bei der Offenlegung von Quellcode
        - Offenlegung nicht vertraulicher Informationen
        - E-Mail-Bombing
        - Request Flooding & DoS/DDoS
        - Fehlende Ratenbegrenzung
        - CSV-Injection

6.4.3 Im Allgemeinen

- pflegen wir einen offenen Dialog, um Probleme zu besprechen, ohne dass eine NDA unterzeichnet werden muss,
- geben wir keine personenbezogenen Daten wie Ihren Namen oder Ihre Kontaktdaten ohne ausdrückliche Genehmigung an Dritte weiter,
- stellen wir sicher, dass das Gespräch im Rahmen der gesetzlichen Bestimmungen vertraulich bleibt,
- sorgen wir dafür, dass wir während des gesamten Prozesses ein vertrauenswürdiger Ansprechpartner für einen vertrauensvollen Austausch sind,

- veröffentlichen wir auf Wunsch Ihren Namen/Alias und eine gewünschte Referenz auf unserer Anerkennungswebsite (Hall of Fame), nachdem eine gültige Schwachstelle gemeldet und der Offenlegungsprozess abgeschlossen wurde. Alle beteiligten Parteien behandeln einander mit Respekt, und es gibt keinen Raum für rechtswidriges Verhalten wie Diskriminierung, Sexismus, Rassismus, Nazismus, Gewaltverherrlichung, Pornografie, Beleidigungen, Verleumdung und üble Nachrede. Im Falle eines Verstoßes in dieser Hinsicht wird MENNEKES auf eine Veröffentlichung verzichten.
- stellen wir sicher, dass Produkt-Schwachstellen in Absprache mit dem zuständigen CSIRT öffentlich gemacht werden.

7 Ende des Prozesses

MENNEKES wird den koordinierten Schwachstellen-/verantwortungsvollen Offenlegungsprozess beenden und den Forscher (sofern nicht anonym eingereicht) ohne unangemessene Verzögerung informieren,

- wenn die Ergebnisse der Schwachstelle unbegründet sind,
- wenn die Schwachstelle eines Produkts, Systems oder Dienstes behoben und ggf. öffentlich gemacht wurde,
- wenn die Schwachstelle durch einen entsprechenden Patch behoben oder gemindert und ggf. öffentlich verfügbar gemacht wurde,
- wenn die Produkt-Schwachstelle öffentlich gemacht wurde und in Absprache mit dem zuständigen CSIRT nicht mehr davon ausgegangen werden kann, dass die Schwachstelle gemindert oder behoben wird.

8 Fragen

Fragen zu dieser Richtlinie oder zum Status einer gemeldeten Schwachstelle sind willkommen. Sie können an psirt@mennekes.org oder csirt@mennekes.org gesendet werden. Wir laden Sie auch ein, uns Vorschläge zur Verbesserung dieser Richtlinie zu unterbreiten.