For the English version please go to page 4

SWD-Richtlinie zur koordinierten Offenlegung von Schwachstellen

Die Stadtwerke Düsseldorf AG (SWD) legt großen Wert auf die Sicherheit ihrer IT-Systeme. Trotz sorgfältigster Implementierung, Konfiguration und Prüfung können dennoch Schwachstellen vorhanden sein. Der Entdecker einer Schwachstelle schafft keine neue Schwachstelle. Wenn ein Entdecker die Existenz einer Schwachstelle jedoch nicht bekannt gibt, ist das keine Garantie dafür, dass ein anderer sie nicht finden wird - oder sie nicht bereits gefunden hat. Entdecker von Schwachstellen können ihre Gründe haben, die Schwachstelle öffentlich zu machen; dabei ist eine koordinierte Offenlegung immer zu bevorzugen.

Wenn Sie also Schwachstellen in IT-Systemen und Webanwendungen der SWD entdecken, informieren Sie uns bitte per E-Mail an security@swd-ag.de. Wir werden dann umgehend Maßnahmen ergreifen, um die gefundene Schwachstelle so schnell wie möglich zu beheben.

Bitte gehen Sie wie folgt vor

- Bevor Sie Ihre Meldung einreichen, sollten Sie sich informieren, welche Fälle außerhalb des Geltungsbereichs unserer SWD-Richtlinie zur koordinierten Offenlegung von Schwachstellen liegen (siehe unten) und nicht im Rahmen dieser Richtlinie bearbeitet werden.
- Senden Sie Ihre Erkenntnisse über die Schwachstelle per E-Mail an security@swd-ag.de. Verschlüsseln Sie Ihre Dokumentation vorzugsweise mit unserem SMIME-Zertifikat, um zu verhindern, dass diese sensiblen Informationen an böswillige Akteure weitergegeben werden. Um die Kommunikation zwischen Ihnen und der SWD zu vereinfachen, verwenden Sie bitte die untenstehende Vorlage.
- Nutzen Sie die Schwachstelle oder das Problem nicht aus, indem Sie z. B. Daten herunterladen, ändern, löschen oder Code hochladen. Sollte dies im Zuge der Entdeckung der Schwachstelle versehentlich erfolgt sein, dokumentieren Sie das bitte in Ihrer Meldung.
- Geben Sie keine Informationen über die Schwachstelle an Dritte oder Institutionen weiter, es sei denn, dies wurde von SWD genehmigt.
- Führen Sie keine Angriffe (oder Handlungen, die als solche gewertet werden könnten) auf unsere IT-Systeme durch, die Infrastrukturen und Personen gefährden, verändern oder manipulieren.
- Führen Sie keine Social Engineering (z.B. Phishing), (Distributed) Denial of Service, Spam oder andere Angriffe gegen die SWD durch.
- Stellen Sie uns ausreichend Informationen zur Verfügung, damit wir das Problem reproduzieren und analysieren können. Geben Sie bitte auch einen Kontakt für Rückfragen an.

Was wir versprechen

- Wir werden versuchen, die Schwachstelle so schnell wie möglich zu schließen.
- Sie erhalten von uns eine Rückmeldung über den Eingang Ihrer Meldung und über Ihre Meldung.

- Wenn Sie sich an die oben genannten Vorgaben der SWD-Richtlinie zur koordinierten Offenlegung von Schwachstellen halten, verpflichtet sich die SWD, keine rechtlichen Schritte gegen Sie einzuleiten. Dies gilt nicht, wenn offensichtlich erkennbare kriminelle oder nachrichtendienstliche Absichten oder Handlungen vorliegen.
- Wir werden Ihre Meldung vertraulich behandeln und Ihre persönlichen Daten nicht ohne Ihre Zustimmung an Dritte weitergeben.
- Wir informieren Sie über den Eingang Ihrer Meldung sowie über die Gültigkeit der Schwachstelle und die Behebung des Problems während des Bearbeitungszeitraums.

Qualifizierte Meldung von Schwachstellen

Jedes Design- oder Implementierungsproblem bei der SWD kann gemeldet werden, das reproduzierbar ist und die Informations- oder IT-Sicherheit betrifft.

Übliche Beispiele sind:

- Cross Site Request Forgery (CSRF)
- Cross Site Scripting (XSS)
- Insecure Direct Object Reference
- Remote Code Execution (RCE) – Injection Flaws
- Information Leakage and Improper Error Handling
- Unauthorized access to properties or accounts
- Data / information leaks
- Possibility of data / information exfiltration
- Actively exploitable backdoors
- Possibility of unauthorized system use
- Misconfigurations

Nicht qualifizierte Schwachstellen

Die folgenden Schwachstellen fallen nicht in den Anwendungsbereich der SWD-Richtlinie zur koordinierten Offenlegung von Schwachstellen:

- Angriffe, die einen physischen Zugriff auf das Gerät oder Netzwerk eines Benutzers erfordern
- Formulare mit fehlenden CSRF-Tokens, es sei denn, die Kritikalität übersteigt die Stufe 5 des Common Vulnerability Scoring System (CVSS)
- Fehlende Sicherheits-Header, die nicht direkt zu einer ausnutzbaren Sicherheitslücke führen
- Verwendung einer Bibliothek, von der bekannt ist, dass sie angreifbar ist, oder von der öffentlich bekannt ist, dass sie schwachstellenbehaftet ist (ohne aktiven Nachweis der Ausnutzbarkeit)
- Berichte von automatischen Tools oder Scans ohne erklärende Dokumentation
- Social Engineering gegen SWD-Mitarbeiter oder -Einrichtungen und deren Auftragnehmer
- Denial-of-Service-Angriffe (DoS/DDoS)
- Bots, SPAM, Massenregistrierung
- Nicht umgesetzte Best Practices (z. B. Zertifikats-Pinning, Security Header)
- Verwendung von anfälligen und „schwachen“ Ciphersuits

Vorlage für einen Bericht über eine Sicherheitslücke

In der Regel reichen die Adresse oder der Uniform Ressource Locator (URL) des betroffenen Systems und eine Beschreibung der Sicherheitslücke aus. Komplexe Schwachstellen können jedoch weitere Erklärungen und Dokumentationen erfordern.

Um eine Schwachstelle an die SWD zu melden, verwenden Sie bitte die folgende Vorlage.

- Titel oder Name der Schwachstelle
- Art der Schwachstelle
- Kurze Erläuterung der Schwachstelle (ohne technische Details) und wie Sie die Schwachstelle gefunden haben
- Betroffenes Produkt, Service, IT-System oder Gerät inkl. Hersteller, Produkt, Version oder Modell
- Art der Ausnutzung der Schwachstelle (aus der Ferne, lokal, Netzwerk, physisch)
- Authentifizierungsinformationen (Pre-Auth, Authentifizierung als Gast, Benutzerrechte (Benutzer, Administrator usw.))
- Benutzerinteraktion (keine Interaktion, geringe Interaktion, mittlere Interaktion, hohe Interaktion)
- Technische Details und Beschreibung der Sicherheitslücke
- Machbarkeitsnachweis
- Darstellung einer möglichen Lösung
- Autor und Kontaktangaben

Wenn Sie eine Veröffentlichung planen, teilen Sie uns dies bitte mit. Gegebenenfalls wird die SWD die öffentliche Bekanntgabe einer bestätigten Schwachstelle mit Ihnen koordinieren. Wenn möglich, würden wir es bevorzugen, dass unsere jeweiligen öffentlichen Bekanntmachungen gleichzeitig erfolgen. Zum Schutz unserer Kunden bittet die SWD Sie, keine Informationen über eine mögliche Schwachstelle in der Öffentlichkeit zu veröffentlichen oder weiterzugeben, bis wir die gemeldete Schwachstelle untersucht, darauf reagiert, sie behoben und die Kunden bei Bedarf informiert haben.

SWD Coordinated Vulnerability Disclosure Policy

Stadtwerke Düsseldorf AG (SWD) attaches great importance to the security of its IT information technology systems. Despite the most careful implementation, configuration and testing, vulnerabilities may still exist. Finders of vulnerabilities do not create vulnerabilities. The fact that one finder does not disclose its existence does not guarantee that another will not find it – or has not already found it. Finders may have reasons to disclose the vulnerability publicly. A coordinated disclosure situation is preferable to one without control.

Therefore, if you discover vulnerabilities in IT information technology systems and web applications of SWD, please inform us via email to security@swd-ag.de. We will then take immediate action to remedy the vulnerability found as quickly as possible.

Please proceed as follows

- Prior to submitting your report, you should find out which cases are outside the scope of our SWD Coordinated Vulnerability Disclosure Policy (see below) and which will not be processed under this policy.
- Email your findings on the vulnerability to security@swd-ag.de. Preferably encrypt your documentation with our SMIME-Certificate to prevent this sensitive information from being disclosed to malicious actors. To streamline communication between you and SWD, please use the template below.
- Do not exploit the vulnerability or problem by, for example, downloading, modifying, deleting data, or uploading code. If this was done inadvertently while discovering the vulnerability, please document this in your report.
- Do not disclose information about the vulnerability to third parties or institutions unless this has been approved by SWD.
- Do not conduct attacks (or actions that could be construed as such) on our IT- systems that compromise, alter, or manipulate infrastructure and people.
- Do not conduct social engineering (e.g., phishing), (distributed) denial of service, spam, or other attacks against SWD.
- Provide sufficient information for us to reproduce and analyze the problem. Also please provide a contact for queries.

What we promise

- We will try to fix the vulnerability as soon as possible.
- We will inform you about the receipt of your report, and about the validity of the vulnerability and the resolution of the problem during the period of processing.
- If you act in accordance with the above instructions of the SWD Coordinated Vulnerability Disclosure Policy, SWD pledges not to initiate legal action against you. This does not apply if there are obviously identifiable criminal or intelligence intentions or actions.
- We will treat your report confidential and will not disclose your personal data to third parties without your consent.

Qualified vulnerability reporting

Any design or implementation issue at SWD can be reported that is reproducible and affects information or IT security.

Common examples include:

- Cross Site Request Forgery (CSRF)
- Cross Site Scripting (XSS)
- Insecure Direct Object Reference
- Remote Code Execution (RCE) – Injection Flaws
- Information Leakage and Improper Error Handling
- Unauthorized access to properties or accounts
- Data / information leaks
- Possibility of data / information exfiltration
- Actively exploitable backdoors
- Possibility of unauthorized system use
- Misconfigurations

Non-qualified vulnerabilities

The following vulnerabilities do not fall within the scope of the SWD Coordinated Vulnerability Disclosure Policy:

- Attacks that require physical access to a user's device or network
- Forms with missing CSRF tokens except criticality exceeds Common Vulnerability Scoring System (CVSS) level 5
- Missing security headers that do not directly lead to an exploitable vulnerability
- Using a library known to be vulnerable or publicly known to be broken (without active evidence of exploitability)
- Reports from automated tools or scans without explanatory documentation
- Social engineering against SWD personnel or facilities and their contractors
- Denial of Service attacks (DoS/DDoS)
- Bots, SPAM, mass registration
- Failure to apply best practices (e.g., certificate pinning, security header)
- Use of vulnerable and "weak" cipher suites/ciphers

Template of a vulnerability report

Usually, the address or Uniform Resource Locator (URL) of the affected system and a description of the vulnerability is sufficient. However, complex vulnerabilities may require further explanation and documentation.

To submit a vulnerability report to SWD, please utilize the following template.

- Vulnerability title or name
- Vulnerability type
- Brief explanation of the vulnerability (without technical details) and how you found the vulnerability
- Affected product, service, IT-system or device incl. manufacturer, product, version, or model
- Exploitation technique (remote, local, network, physical)
- Authentication type (pre-auth, authentification as guest, user privileges (user, admin, etc.)
- User Interaction (no interaction, low interaction, medium interaction, high interaction)
- Technical details and description of the vulnerability
- Proof of Concept
- Demonstration of a possible solution
- Author and contact details

If you have any plans for public disclosure, please let us know. If applicable, SWD will coordinate public notification of a validated vulnerability with you. If possible, we would prefer that our respective public disclosures be posted simultaneously. To protect our customers, SWD requests that you do not post or share any information about a potential vulnerability in any public setting until we have researched, responded to, and addressed the reported vulnerability and informed customers if needed.