Vulnerability Disclosure Policy der Bundeswehr (VDPBw)

Umsetzung an der Universität der Bundeswehr München (UniBw M)

Die Bundeswehr legt größten Wert auf die Sicherheit ihrer IT-Systeme. Trotz sorgfältigster Implementierung, Konfiguration und Tests können dennoch Schwachstellen vorhanden sein.

Security Policy:

Sollten Sie Schwachstellen in IT-Systemen und Webanwendungen der UniBw M entdecken, bitten wir Sie uns darüber zu informieren. Wir werden dann umgehend Maßnahmen ergreifen, um die gefundene Schwachstelle so schnell wie möglich zu beheben.

Die VDPBw darf nicht ohne Einwilligung der Bundeswehr dazu verwendet werden, um in Programmen Dritter Schwachstellenmeldungen aufzubereiten oder weiter zu vermitteln.

Gehen Sie wie folgt vor:

- Informieren Sie sich vor Ihrer Meldung über die Fälle, die nicht in den Geltungsbereich unserer VDPBw fallen und in diesem Rahmen nicht bearbeitet werden.
- Informieren Sie den Informationssicherheitsbeauftragten der UniBw M (isb@unibw.de)
- Nutzen Sie die Schwachstelle oder das Problem nicht aus, indem Sie beispielsweise Daten herunterladen, verändern, löschen oder Code hochladen.
- Geben Sie Informationen über die Schwachstelle nicht an dritte Personen oder Institutionen weiter, außer dies wurde durch die Bundeswehr freigegeben.
- Führen Sie keine Angriffe auf unsere IT-Systeme durch, die Infrastruktur und Personen kompromittieren, verändern oder manipulieren.
- Führen Sie keine Social-Engineering- (z.B. Phishing), (Distributed) Denial of Service-, Spam- oder andere Angriffe auf die Bundeswehr durch.
- Stellen Sie uns hinreichend Informationen zur Verfügung, damit wir das Problem reproduzieren und analysieren können. Stellen Sie auch eine Kontaktmöglichkeit für Rückfragen bereit.

In der Regel ist die Adresse oder die URL (Uniform Resource Locator) des betroffenen Systems und eine Beschreibung der Schwachstelle hinreichend. Komplexe Schwachstellen können aber weitere Erklärungen und Dokumentation erfordern.

Was wir versprechen:

- Wir versuchen die Schwachstelle so schnell wie möglich zu schließen.

- Sie erhalten von uns eine Rückmeldung zum Eingang Ihrer Meldung und auf Ihren Bericht.

- Handeln Sie gemäß den oben genannten Anweisungen der Security Policy der Bundeswehr, werden die Strafverfolgungsbehörden im Zusammenhang mit Ihren Erkenntnissen nicht informiert. Dies gilt nicht, wenn erkennbar kriminelle oder nachrichtendienstliche Absichten verfolgt werden.

- Wir werden Ihren Bericht vertraulich behandeln und Ihre personenbezogenen Daten nicht ohne Ihre Zustimmung an Dritte weitergeben.

- Wir werden Sie über den Eingang Ihrer Meldung informieren, darüber hinaus ebenso über die Validität der Schwachstelle/IT-Sicherheitslücke und die Behebung des Problems während des Zeitraums der Bearbeitung.

Qualifizierte Meldung von Schwachstellen:

Jedes Design- oder Implementierungsproblem bei der Bundeswehr kann gemeldet werden, das reproduzierbar ist und die Sicherheit beeinträchtigt.

Häufige Beispiele sind:
- Cross Site Request Forgery (CSRF)
- Cross Site Scripting (XSS)
- Insecure Direct Object Reference
- Remote Code Execution (RCE) - Injection Flaws
- Information Leakage an Improper Error Handling
- Unbefugter Zugriff auf Eigenschaften oder Konten
- Daten-/Informations- Leaks
- Möglichkeit der Exfiltration von Daten / Informationen
- Aktiv ausnutzbare Hintertüren (Backdoors)
- Möglichkeit einer unautorisierten System-Nutzung
- Fehlkonfigurationen

Nicht-qualifizierte Schwachstellen

- Angriffe, die einen physischen Zugriff auf das Gerät oder Netzwerk eines Benutzers erfordern
- Formulare mit fehlenden CSRF-Token (Ausnahme: Die Kritikalität übersteigt das CVSS) Stufe 5.).
- Missing security headers, die nicht direkt zu einer ausnutzbaren Schwachstelle führen.
- Die Verwendung einer als anfällig oder öffentlich als gebrochen bekannte Bibliothek (ohne aktiven Nachweis der Ausnutzbarkeit).
- Berichte von automatisierten Tools oder Scans ohne erklärende Dokumentation.
- Social Engineering gegen Personen oder Einrichtungen der Bundeswehr sowie deren Auftragnehmer.
- Denial of Service-Angriffe (DoS/DDoS (Distributed Denial of Service)).
- Bots, SPAM, Massenregistrierung.
- Keine Einreichung von Best Practices (z.B. certificate pinning, security header)
- Verwendung von anfälligen und „schwachen“ Cipher-Suites / Chiffren.

Formatvorlage einer Schwachstellenmeldung:

1. Titel / Bezeichnung der Schwachstelle
2. Schwachstellentypus
3. Kurzerklärung der Schwachstelle (ohne technische Details)
4. Betroffenes Produkt / Dienst / IT-System / Gerät
    1. Hersteller
    2. Produkt
    3. Version / Modell
5. Exploitationtechnik
    1. Remote
    2. Local
    3. Netzwerk
    4. Physisch

6. Authentication-Typ
    1. Pre-Auth
    2. Authentification Guest
    3. Benutzer-Privilegien (Moderator / Manager / Admin)
7. Benutzerinteraktion
    1. No User
    2. Low User Interaction
    3. Medium User Interaction
    4. High User Interaction
8. Technische Details und Beschreibung der Schwachstelle
9. Proof of Concept
10. Aufzeigen einer Lösungsmöglichkeit
11. Autor und Kontaktdaten

Kontakt:

Universität der Bundeswehr München
Informationssicherheitsbeauftragte
+49 89 6241 2092
isb@unibw.de