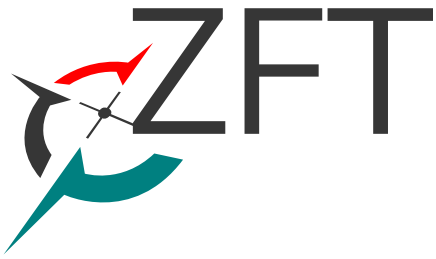

Ergebnisreport Untersuchung «Ticketcontrol»

durchgeführt von

ZFT.COMPANY GmbH

Autoren

Dr. André Zilch,
Sven Fassbender,
Martin Tschirsich

Version: 1.1
Datum: 25.01.2022

Inhaltsverzeichnis

1. Zusammenfassung

Die aus dem Internet zugängliche Schnittstelle «Ticketcontrol» zum nationalen Schwarzfahrerregister dient der Erfassung von Personendaten, welche im Zusammenhang mit einem Schwarzfahrerdelikt erhoben werden. Ziel ist es Personen, die wiederholt schwarzfahren, mithilfe des Registers schneller zu identifizieren. Die Prozesse zur Erhebung der Daten wurden durch dieses Register schweizweit vereinheitlicht. Die Einführung des nationalen «Schwarzfahrerregisters» geht auf einen Parlamentsbeschluss des Jahres 2015 zurück. Über die «Ticketcontrol»-Schnittstelle können betroffene Personen Belege hochladen zum Nachweis, dass sie einen gültigen Fahrausweis besitzen. Zudem können kleine Verkehrsverbünde in standardisiertem Format registrierte Schwarzfahrer melden.

Bereits eine kursorische Untersuchung der Schnittstelle hat einen kritischen Sicherheitsmangel aufgedeckt:

- Aufgrund einer sogenannten «Insecure-Direct-Object-Reference» (IDOR-Schwachstelle) waren über diese Schnittstelle hochgeladene Daten nicht gegen Zugriff aus dem Internet gesichert.

Damit war das Ziel, «vertrauliche Tatsachen und Informationen gegen den Zugang und die Kenntnisnahme durch Unbefugte wirksam» zu schützen, nicht erreicht.

Die gemeldete Schwachstelle wurde umgehend durch den Betreiber behoben. Für einen sicheren Weiterbetrieb der Schnittstelle «Ticketcontrol» ist eine regelmässige Prüfung der Schutzmassnahmen empfehlenswert.

Der identifizierte Mangel wurden den Verantwortlichen in einem Coordinated-Disclosure-Verfahren mitgeteilt. Ziel war, dass der identifizierte Mangel durch die Verantwortlichen behoben wird. Eine Veröffentlichung des Reportes erfolgt in Abstimmung mit den Verantwortlichen.

2. Übersicht der Befunde

Nr.	Titel	Risiko
3.1	Insecure-Direct-Object-Reference	Hoch

3. Befunde

Dieser Abschnitt beinhaltet die detaillierte Beschreibung der identifizierten Schwachstelle.

3.1. Insecure-Direct-Object-Reference

Klasse	Zugriffskontrolle
Risiko	Hoch

Eine fehlende Zugriffskontrolle erlaubt einem Angreifer aus dem Internet über eine «Insecure-Direct-Object-Reference» (IDOR-Schwachstelle[1]) den Zugriff auf vertrauliche Daten.

In mindestens einem Fall kann über «Ticketcontrol» auf vertrauliche Informationen des Registers zugegriffen werden, da für diesen Zugriffspfad keine Zugriffskontrolle implementiert wurde.

Die clientseitig im Browser eines nicht authentisierten Benutzers ausgeführte Webanwendung lädt Ressourcen wie JavaScript- oder Bilddateien über folgenden Zugriffspfad per HTTP-GET-Anfrage unter Angabe einer numerischen Kennung im URL-Pfad:

```
GET /data/docs/de/1975/iscroll.js?v=1.0 HTTP/2
Host: www.ticketcontrol.ch
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Accept-Encoding: gzip, deflate
Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7
```

Augenscheinlich handelt es sich bei der numerischen Kennung um einen fortlaufenden Dokumenten-Index. Der Zugriff gelingt ohne Angabe von Authentifizierungsmerkmalen. Einfaches Inkrementieren oder Dekrementieren der numerischen Kennung erlaubt einem nicht-authentisierten Angreifer aus dem öffentlichen Internet den Zugriff auf vertrauliche Daten.

Empfehlungen

Alle Anfragen müssen serverseitig vor der Weiterverarbeitung einer Berechtigungs- bzw. Autorisierungsprüfung unterzogen werden. Bei der Vergabe von Berechtigungen sollte nach dem *Least-Privilege-Prinzip*[2] verfahren werden.

[1] Portswigger, Insecure direct object references (IDOR), https://portswigger.net/web-security/access-control/idor, zuletzt besucht am 20.01.2022

[2] Cybersecurity & Infrastructure Security Agency, Least Privilege, https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege, zuletzt besucht am 20.01.2022