

# **Lokalisten: identity problems**

## **“Hyjacking” other profiles ~~is~~ was so much fun!**

**By Valentin Höbel. Mail to [valentin@xenuser.org](mailto:valentin@xenuser.org)  
(February 2010)**

- I. What is this document about?**
- II. About Lokalisten**
- III. The “Hyjacking” part**
- IV. Summary**
- V. Sources and other stuff**

### **I. What is this document about?**

This document explains the security issues the German social networking website Lokalisten had this Friday (12<sup>th</sup> February 2010).

### **II. About Lokalisten**

Lokalisten is one of the most used social networking sites in Germany. Having millions of members, this service provides basic social networking features and a focus on local communities/cities.

### **III. The “Hyjacking” part**

Lokalisten.de is one of the websites many German people open up when they start their web browsers for the first time of the day. It is very popular in Munich since it provides features which help you to organize local event and get in touch with people.

When I entered the class room (Berufsschule, you can translate it with vocational school) this morning one of my class mates screamed since he suddenly had access to another profile/identity at Lokalisten.

I was curious, booted a PC and had a look myself: Indeed, each time you access Lokalisten and refresh the page, you are logged in as someone else. This happened the first time at this day and definitely did not occur the evening the day before.

We started to play around with it and were able to view some data like the provided data

of the foreign identity (like the full name), view his friends and their data, view their birthday dates and various other things. Reading the private messages of the current user or changing the status, deleting photos and removing friends from the buddy list was not possible.

So this issue was not critical but still something which can annoy the Lokalisten.de users.

The funny part about this thing is that when you logged in, the next person to access Lokalisten basically had access to your profile and when he/she clicked on a link, every other person to follow would see his/her data and so on. This means that either the school proxy or Lokalisten was caching something which was important for authenticating the user (maybe a cookie or even a session file). Since we all browsed the web with the same IP address, we were able to see each other profiles. More than 40 people were online when this bug was discovered, so you can believe that most people were shocked since they were concerned about their privacy.

This problem did not occur when you log in from a place where you are the only one with the external WAN IP.

After I contacted the school proxy administrator, I found out that the configuration of their networking and proxy service was not changed. This indicated that the problem was caused by something the vendor did.

I contacted Lokalisten and assumed that some changes were applied during the night. After a few hours the problem was fixed.

#### **IV. Summary**

This security issue didn't reveal many information about their users so I guess you can mark it as non-critical. Lokalisten responded very fast, tracked down the issue and was able to solve this problem. In the end something was cached by a specific proxy software (being used in several companies and schools) which caused the problem.

#### **V. Sources and other stuff**

Thx going out to Matthias Pressler for screaming when he discovered that he suddenly got logged in as someone else.

Thx also going out to Lokalisten and their fast response.

#### **Chronic (12<sup>th</sup> February 2010):**

7:40 am: Discovery of the issue

10:22 am: Problem reported to vendor

11:00 am - 12:00 am: Problem solved

You may publish this document and copy stuff in any way you like.

Valentin Höbel

valentin@xenuser.org

<http://www.xenuser.org>