stashcat

Exposure of Private Personal Information to an Unauthorized Actor (CWE 359)

Jens van Laak

May 18, 2020

Stashcat is an instant messenger that is advertised to be safe and conformant to data protection regulations of the European Union. According to the vendor stashcat is used by German State Police in Niedersachsen and in Hessen and the German Armed Forces.

The API of Stashcat exposes in the listing of users private personal information of other users that are not shown in the application. Among others are:

1. email address
2. last login time
3. list of companyID (which is the grouping mechanism)

Using the sessionID of his own session an attacker can forge a URL to retrieve the complete list of all users with each respective data block.

1 Overview

Vendor Stashcat Gmbh (owned by heinekingmedia GmbH)

Vendor Website https://www.stashcat.com

Product stashcat

Version ≤ 3.9.1

Product Website https://app.stashcat.com

Impact Information Disclosure

Attack Vector direct HTTPS request to API server with SessionID

2 Description

Stashcat uses an API to communicate with the system's server. Most of the requests are handled via HTTPS GET, POST and OPTIONS requests.

Two parameters – client_key and device_id – build the sessionID and are sent in each HTTPS request as parameters. The sessionID stays valid over a longer period of time (days), if the user does not explicitly log off. The log off function is *not* available in an easy way.

The list of users is retrieved from the system when the user searches for other users. This is done with a POST request to the URL: https://api.stashcat.com/users/listing using the parameters client_key, device_id, offset and limit. The parameters company, key_hashes, search and sorting are used by the webapplication but they are optional.

The data transmitted to the client is the requested list in JSON format with the following fields: active, deactivated, email, first_name, image, last_login, manager, online, public_key, read_only, status, time_joined, and role. The last one is a list of companies, which is a grouping mechanism in stashcat.

3 Description of the attack

An attacker needs access to a user account. He can then retrieve the client_key and device_id using the developers tool of the browser[1]. He can also get them by analysing his own web traffic after dumping the SSL keys of the browser or by using a SSL gateway. This is easy to do on private devices that are under full controll of the attacker.

The attacker can then forge and retrieve the respective URL with changed parameters. The optional ones can be dropped and the limit can be increased to a value higher than the estimated number of users[2]. This gives a complete list of all users with the complete dataset of each.

4 Impact

The data block of each user contains data that is not needed for the functionallity of the application in the context of the user directory visible to the user.

Especially for the email address and last login time there is no user consent to share this with other users.

The user can keep the sessionID valid by not logging off the system and use this sessionID to automate the regular retrieval of the full list. This gives opportunity to a wide range of analyis:

1. reveal the exact number of users
2. get all email addresses with firstname and name

[1]Normally started by pressing [F12].

[2]The system accepts 85.000 as a limit.

3. reveal changes of data by comparison to formerly stored data
4. reveal the group structures
5. identify the admin accounts
6. track activity of users