Trovebox 4.0.0-rc6 SQL Injection / Bypss / SSRF

May 02, 2018

Exploit Collector

Trovebox versions 4.0.0-rc6 and below suffer from authentication bypass, server-side request forgery, unsafe token generation, nd remote SQL injection vulnerabilities.

MD5 | `4f1421667f2b120bcf321218e53f6bbe`

Download

```
    Advisory: Trovebox - Authentication Bypass, SQLi, SSRF
 Release Date: 2018/04/30
       Author: Robin Verton (robin.verton@telekom.de)
          CVE: requested

  Application: Trovebox <= 4.0.0-rc6
         Risk: Critical
Vendor Status: A fix was released on github.

Overview:

  "Trovebox is software that helps you manage, organize and share photos. It
  includes web and mobile apps for Android and iOS. The goal of Trovebox is to
  be software which people love to use and helps them preserve their digial
  media files." [1]

  Multiple vulnerabilities were identified in the current release of Trovebox
  allowing to bypass authentication, inject SQL code or access local services
  and hosts.

Details:

  1) Authentication bypass via type juggling

    Trovebox puts JSON serialized data in a table column and deserializes this
    data when accessing it. If an accessed dictionary key can not be found in
    this result, bool(false) is returned. The passwordReset() function makes use
    of an unsafe comparison which allows to pass this check if there is no
    active token saved for the user:

      //ApiUserController.php, L89
      $user = new User;
      $token = $_POST['token'];
      $password = $_POST['password'];
      $passwordConfirm = $_POST['password-confirm'];
      $tokenFromDb = $user->getAttribute('passwordToken');
      if($tokenFromDb != $token)
        return $this->error('Could not validate password reset token.', false);

    Note that this will always reset the password for the owner/admin account,
    because the email address is not used here. By using an empty string ("") as
    the password token, the password can then be changed.
```

```
  2) Unsafe password reset token generation

    The password reset token generation is not random enough:

      //ApiUserController.php, L59
      $token = md5(rand(10000,100000));

    There are only 90.000 different tokens which is trivial to crack in a
    short time frame.


  3) SQL injection in album list function

    The buildQuery() function in DatabaseMySql.php fails to validate the 'album'
    parameter.

    Example: /photos/album-1'[SQL]/list
    Example: /photos/album/list?album=1'[SQL]


  4) Server-Side request forgery in webhook subscription functionality

    The webhook subscribe function does not sufficient filter the passed
    callback url, thus allowing an authenticated user to access internal services
    and hosts.

    Example contacting a local SSHd:

      $ curl -XPOST pwnbox:8080/webhook/subscribe \
      -d "mode=GET&topic=a&callback=dict://127.0.0.1::22/?" \
      --cookie "PHPSESSID=jm6adsphu75m8kna0drkhj9nj4"
      The verification call failed to meet requirements. Code: 0, Response: SSH-
      2.0-OpenSSH_6.6.1p1 Ubuntu-2ubuntu2.8 Protocol mismatch.
      , Expected: 5a7f6cfc81a78, URL: dict://127.0.0.1:22/?mode=GET&topic=a&challenge=5a7f6cfc81a78


References:

    [1]: https://github.com/photo/frontend

Disclosure Timeline:
```

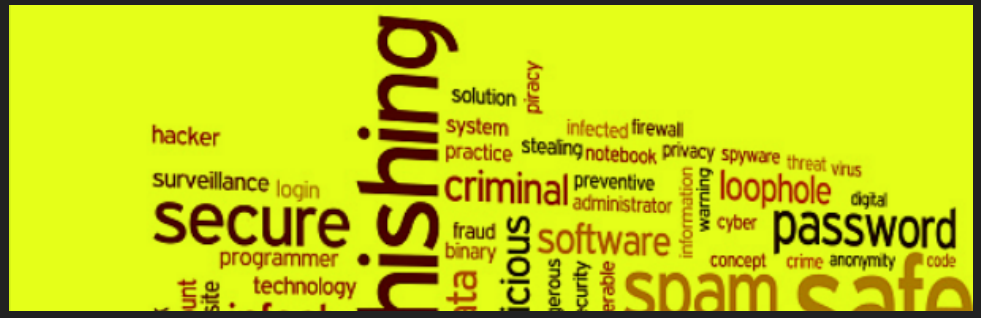
```
About Telekom Security:

  Telekom Security is the security provider for Deutsche Telekom and Deutsche
  Telekom customers.

  https://security.telekom.com
  https://github.com/telekomsecurity
  http://www.sicherheitstacho.eu

  https://telekomsecurity.github.io/2018/04/trovebox-vulnerabilities.html
```

Source: packetstormsecurity.com

Related Posts

Exploit Collector

Popular Posts



Linux/x86 Read /etc/passwd Shellcode

Exploit Collector

Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.

Attackers can exploit this vulnerability to execute arbitrary code in the ...

WhatsApp 2.18.31 iOS Memory Corruption

WhatsApp version 2.18.31 on iOS suffers from a remote memory corruption vulnerability.

Exploit Collector

Archive