Whole Vibratissimo Smart Sex Toy XSS / Disclosure / Authentication

February 02, 2018

Exploit Collector

Multiple versions of Whole Vibratissimo Smart Sex Toy suffer from credential disclosure, exposed administrative interface, cleartext storage of passwords, unauthenticated bluetooth LE connection, and other vulnerabilities. These devices screw you in more way than one.

MD5 | `03c724a03de35ee0666055d71102b9f1`

```
We have published an accompanying blog post to this technical advisory with
further information:

https://www.sec-consult.com/en/blog/2018/02/internet-of-dildos-a-long-way-to-a-vibrant-future-from-iot-to-iod/i


SEC Consult Vulnerability Lab Security Advisory < 20180201-0 >
=======================================================================
             title: Multiple critical vulnerabilities
           product: Whole Vibratissimo Smart Sex Toy product range
 vulnerable version: <6.3 (iOS), <6.2.2 (Android), <2.0.2 (Firmware)
     fixed version: 6.3 (iOS), 6.2.2 (Android), 2.0.2 (Firmware)
        CVE number: -
            impact: critical
          homepage: http://www.vibratissimo.com
             found: 2017-10-01
                by: W. Schober (Office Vienna)
                    SEC Consult Vulnerability Lab

                    An integrated part of SEC Consult
                    Bangkok - Berlin - Linz - Luxembourg - Montreal - Moscow
                    Kuala Lumpur - Singapore - Vienna (HQ) - Vilnius - Zurich

                    https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"Control with Vibratissimo your AMOR Toy on your smartphone and get even more
features by the app. With Vibratissimo you are open to new and exciting
opportunities, whether you are in the same room or on different continents."

Source: http://www.vibratissimo.com/en/index.html


Business recommendation:
------------------------
SEC Consult highly recommends to update the app to the newest version available
in the appstore. Furthermore the password, which was used within the app,
should be changed immediately. If the password was used for multiple services,
all passwords should be changed. To get rid of issue number 3 (Unauthenticated
```

Exploit Collector

```
---------------------------------
1) Customer Database Credential Disclosure
The credentials for the whole Vibratissimo database environment were exposed on
the internet. Due to the fact, that the PHPMyAdmin interface was exposed as well,
an attacker could have been able to connect to the database and dump the whole
data set. The dataset contains for example the following data:

- Usernames
- Session Tokens
- Cleartext passwords
- chat histories
- explicit image galleries, which are created by the users themselves


2) Exposed administrative interfaces on the internet
An administrative interface for databases was available without any filtering to
the whole internet. In combination with other vulnerabilities an attacker
could have been able to get access to the whole database data and even take over
the server.


3) Cleartext Storage of Passwords
The user passwords were stored unhashed in cleartext in the database.
If an attacker gained access to the database (e.g. via credential disclosure),
he could have been able to retrieve the plaintext passwords of users and abuse
their privileges in the system.


4) Unauthenticated Bluetooth LE Connections
The sex toys are connected without prior authentication to the app, which is the
standard use case. For example one of the identified Bluetooth services allows
to read the current device temperature. Other services, which can be
accessed without prior authentication are:

-) Setting the "intensity" of the current vibration pattern
-) Reading various values (Temperature, etc)


5) Insufficient Authentication Mechanism
The android application is using a type of authentication, which is against
known best practice. The username and password are sent with every
request to the server to authenticate and authorise the request. There is no
session management implemented. However, the authentication credentials are
```

```
allows an attacker to get access to restricted functions and resources. In this
case a user is able to set a profile picture by uploading a provided image. The
image is stored on the Vibratissimo server and renamed. All images are renamed
by incrementing a global number and assigning this number as the name of the
image (e.g 200.png). An attacker is now able to iterate through those images and
dump personal user images containing partially explicit content. The image can
even be accessed if the profile has been set to "hidden" by the user.


7) Missing Authentication in Remote Control
The mobile apps allow their users to use a feature called quick control.
This feature allows to send a link with a unique ID to an email address or a
telephone via SMS to get direct control of the sex toy over the internet.
This wouldn't be a problem in general if the link containing the unique
ID would be random and long enough. Furthermore, it would be quite useful
if the receiving user must confirm the remote control before being
controlled by the other user. Unfortunately this is not the case.

The IDs are again a global counter, which just gets incremented by one
everytime a new quick control link is created. An attacker can guess
this ID easily and therefore control the victim's sex toy directly
over the internet.


8) Reflected Cross-Site Scripting
An endpoint, which handles remote control links, returns unfiltered
user input resulting in reflected XSS attacks. With reflected cross-site
scripting, an attacker can inject arbitrary HTML or JavaScript code into the
victim's web browser. Once the victim clicks a malicious link, the attacker's
code is executed in the context of the victim's web browser. As a result, the
attacker is able to execute arbitrary client-side JavaScript code, for example
to deface the website or steal user credentials. In addition, users of the site
can become victims of browser exploits and JavaScript trojan horses.


Proof of concept:
-----------------
1) Customer Database Credential Disclosure
During the evaluation a .DS_STORE file was found on the webserver of
Amor Gummiwaren GmbH. A .DS_STORE file typically contains a listing of all the
sub-directories in the current directory, including various different custom
attributes for the OSX operating system. In this directory many subdirectories
and files were identified.
```

```
In combination with the exposed phpmyadmin interface an attacker was able to dump
the whole customer database containing sensitive information.


2) Exposed administrative interfaces on the internet
The PHPMyAdmin interface was accessible by everyone without any restrictions
by visiting the following URL

http://www.vibratissimo.com/phpmyadmin/

In combination with the information disclosure vulnerability, which discloses
the database credentials, an attacker could have been able to connect to the
database and extract/dump the available tables including sensitive user
information (such as passwords).


3) Cleartext Storage of Passwords
The password entries of the user were stored in plaintext in the database. As we
don't want to put users at risk and the vulnerability is self explaining a
detailed proof-of-concept is not included in the advisory.


4) Unauthenticated Bluetooth LE Connections
The Bluetooth LE connection between the smartphone and the vibrator, which is
used to control the vibrator is insecure in multiple ways, which leaves the
connection open for eavesdropping, replay-attacks and vulnerable to MitM attacks.

Bluetooth LE offers the following pairing methods:
- No Pairing
- Just Works(TM)
- Out of Band (OOB) Pairing:
- Passkey
- Numeric Comparison

Every available pairing method has its up- and downsides, except the
"No Pairing" method, which is offering only downsides. The reason to use the
"no pairing" is to offer the user simplicity. Furthermore, all the other
methods require some kind of input or interaction by the user, which can't be
offered by the tested devices. The tested device used the "no pairing" method
exclusively. This allows an attacker to query the device for information or
write data to the device. An attacker is therefore able to control the sex toy
remotely if he is in range.
```

```
connection. A request to the API looks as follows:


GET
/userManager.php?action=getUser&password=$clearTextPassword&user_login=$ClearTextUsername
HTTP/1.1
Host: www.vibratissimo.com


6) Insecure Direct Object Reference
The profile pictures of a user are uploaded to the following folder:

https://www.vibratissimo.com/userPictures/$ID.png

The profile pictures can be accessed without prior authentication and even
if the profile has been set to "hidden" by the user.


7) Missing Authentication in Remote Control
For this vulnerability a setup with 3 devices was prepared:

-) The victim
-) The sex toy connected to the victim via Bluetooth
-) The attacker

The victim is directly connected via Bluetooth to the sex toy and creates a
quick control link for his friend. This creates the following link as an example:

https://vibratissimo.com/quickControl.php?id=11359

An attacker can now launch the app and create a quick control link and send the
link to himself. He receives the following link:

https://vibratissimo.com/quickControl.php?id=11360

The attacker can now just decrement the ID in the link by one to get immediate
and direct access to the victim's sex toy.


8) Reflected Cross-Site Scripting
To demonstrate the vulnerability, it is enough to open the following link
in an arbitrary browser:
```

```
Vulnerable / tested versions:
-----------------------------
Vibratissimo <6.3 (iOS), <6.2.2 (Android), <2.0.2 (most up to date version in
October 2017)


Vendor contact timeline:
------------------------
2017-11-08: Contacting CERT-Bund via certbund@bsi.bund.de and handing
            over a detailed vulnerabiliy description. Furthermore,
            asking for help in the process of setting up a secure
            communication channel with the vendor.
2017-11-09: CERT-Bund responds that they securely transmitted the
            information to Amor GmbH and explained them which
            measures should be taken immediately. Furthermore, a
            telephone conference hosted by CERT-Bund, between Amor GmbH
            and SEC Consult is scheduled.
2017-11-09: CERT-Bund responds that the configuration file containing
            the database credentials got removed and the access to
            phpmyadmin is now restricted.
2017-11-27: Transmitting the advisory to Groenewold - new media e.K.,
            CERT-Bund and Amor GmbH over an encrypted channel, which
            was setup by CERT-Bund (S/MIME).
2017-11-30: A telephone conference, hosted by CERT-Bund, was held to remove
            ambiguities and to get feedback from Amor GmbH and
            Groenewold - new media e.K.
2017-12-04: Transmitting the advisory with the adaptions from the last
            call to Groenewold - new media e.K., CERT-Bund and Amor GmbH
            over an encrypted channel, which was setup by CERT-Bund (S/MIME).
2018-01-03: Added vulnerability No. 7 and 8 to the advisory and transmitting
            the advisory with the adaptions to Groenewold - new media e.K.,
            CERT-Bund and Amor GmbH.
2018-01-16: Telephone conference between all parties to discuss details about
            identified vulnerabilities. Furthermore, SEC Consult requested
            affected and fixed versions.
2018-01-23: Telephone conference discussing advisory & blog release for 1st
            February.
2018-02-01: Public advisory release.


Solution:
---------
Vibratissimo immediately removed the configuration file containing the credentials
```

```
-Insufficient Authentication Mechanism (Issue 5)
-Insecure direct object reference (Issue 6)
-Missing Authentication in Remote Control (Issue 7)
-Reflected Cross-Site Scripting (Issue 8)


The mobile apps have to be updated. The current version, were most of the
vulnerabilities are fixed are:
-) Android 6.2.2
-) iOS 6.3

Furthermore it is highly recommended that the password of the application should
be changed. To get rid of the Unauthenticated Bluetooth LE Connections (Issue 4)
the firmware has to be updated by Amor Gummiwaren GmbH. Therefore a user has to
contact Amor Gummiwaren GmbH (info@amor.ag)


Workaround:
-----------
No workaround available.


Advisory URL:
-------------
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html


~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

SEC Consult Vulnerability Lab

SEC Consult
Bangkok - Berlin - Linz - Luxembourg - Montreal - Moscow
Kuala Lumpur - Singapore - Vienna (HQ) - Vilnius - Zurich

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult. It
ensures the continued knowledge gain of SEC Consult in the field of network
and application security to stay ahead of the attacker. The SEC Consult
Vulnerability Lab supports high-quality penetration testing and the evaluation
of new offensive and defensive technologies for our customers. Hence our
customers obtain the most current information about vulnerabilities and valid
```

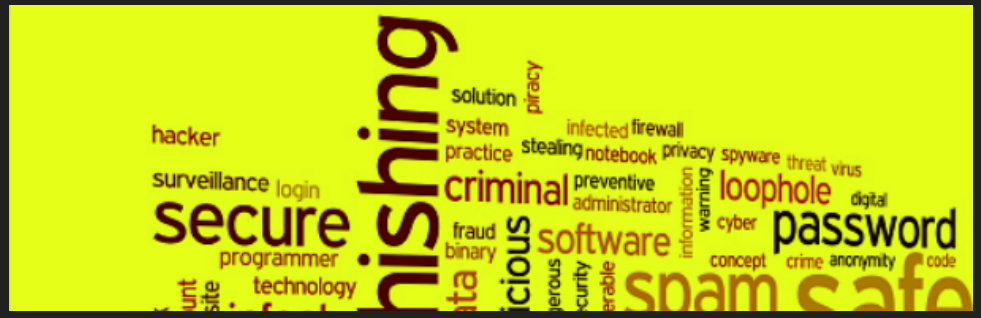
```
Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices https://www.sec-consult.com/en/about-us/index.html
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec_consult

EOF W. Schober / @2018
```

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