ESET Research white papers

TLP: WHITE

SEX IN THE DIGITAL ERA

HOW SECURE ARE SMART SEX TOYS?

Authors:
Denise Giusto
Cecilia Pastorino

CONTENTS

Authors:
Denise Giusto
Cecilia Pastorino

February 2021

INTRODUCTION

As IoT (Internet of Things) devices continue to seep into our homes and offer an increasingly wide range of features, new concerns are beginning to arise about the security of the data processed by these devices. Though they have been subject to countless security breaches leading to the exposure of people's login details, financial information, and geographical location, among others, there are few kinds of data with more potential to harm users, if published, than those relating to their sexual behavior.

With new models of smart toys for adults entering the market all the time, we might imagine that progress is being made in strengthening the mechanisms to ensure good practices in the processing of user information. However, our research shows that we are a long way from being able to live out our sexuality through digital media without exposing ourselves to the risk of cyberattack. Today, these findings are more relevant than ever, since we are seeing a *rapid rise in sex toy sales* as a reflection of the current health situation around the world and the social distancing measures related to COVID-19.

Though many experts have devoted time to identifying and reporting security flaws within this industry, with every passing year these devices incorporate an ever wider range of features: Group chats, multimedia messages, videoconferencing, synchronization with lists of songs or audio books, and much more. Each time their code is re-engineered, some vulnerabilities are corrected, new vulnerabilities may be created, and many more remain unchanged in the updated versions.

So, how secure are adult toys right now? Have the necessary precautions been taken to protect people's data and privacy? These are some of the concerns we address in the course of this whitepaper. We will analyze the increasingly important role played by these types of devices and the vulnerabilities in some of them, placing an emphasis on the importance of demanding—as informed consumers—that best practices and standards are applied to these products in order to ensure that our data is secure and we are unharmed.

THE EVOLUTION OF SEX TOYS

Many consumers see adult toys as a new trend resulting from the new, inescapable fusion of society and technology in the computer era, but in reality these devices have been around for more than a century. In her book *The Technology of Orgasm: Hysteria, the Vibrator, and Women's Sexual Satisfaction*, Rachel P. Maines describes how her research led her to find advertisements for vibrators in popular magazines dating back as far as 1906.

In the early days, embedded in a context where all female sexual behavior that could not be understood from a male-centric perspective was considered unhealthy, these devices were promoted as medical devices designed to cure "female hysteria", otherwise known as "disease of the uterus", which was believed to be a chronic disorder common among women. The treatment for this "ailment" was "known" as far back as the year 1600 and revolved around genital massages carried out by a physician or midwife, culminating in a climax or "hysterical paroxysm": The female orgasm.

So, according to Maines, the first vibrators emerged as a capitalist mechanism to maximize the number of patients that could be treated per day, by reducing the average time needed for each consultation—which had previously been something like an hour—to about ten minutes. This analysis *is disputed*. Fifteen years after the first electromechanical vibrator was invented (in the 1880s), dozens of new manufacturers were producing models powered either by cable or battery.

Although the vibrator's original development is associated with the denial of women's sexuality, its arrival brought with it the possibility of self-discovery for many, at a time when masturbation was considered an abnormal behavior. Alongside the revolution brought about by feminist movements, as well as the growth of the pornography industry, new shapes, materials, and features were added to the original vibrators, which evolved from being seen as medical devices and became a form of sexual liberation.

In recent decades, advances in these devices have been boosted by advances in technology: In the 2000s, there was a new wave of devices featuring remote controlling via infrared connectivity. By 2010, it was possible to find devices locally controlled by apps. And now, in 2020, and indeed for the last few years, it has been possible to find devices that can be connected to other devices across the internet to communicate over a long distance.

CHARACTERISTICS OF SMART SEX TOYS

With the emergence of the IoT, many manufacturers have entered the sexual pleasure market by integrating the ability to control devices through mobile apps as well as adding web-based interconnectivity. There are currently numerous different apps available, each of which offers the ability to control a wide range of models.

In terms of their architecture, most of these devices can be controlled via Bluetooth Low Energy (BLE) from an app installed on a smartphone. The main advantages of this protocol are that it has very low power requirements, communications are within an acceptable range, there is interoperability among chipset manufacturers, and it all comes in a very compact size. As a result, a lot of smart devices for the home, health, car, and even sex toy fields, use BLE between the device and the app that controls it.

Like Bluetooth, BLE operates on the 2.4 GHz ISM band. However, unlike standard Bluetooth, BLE stays in sleep mode all the time, except when a connection is initiated. Also, the actual connection times themselves are just a few milliseconds, unlike Bluetooth, which takes more than 100 milliseconds.
On BLE networks, devices are classed as either central or peripheral. Central devices (smartphones, computers, etc.) have more processing capacity and are responsible for controlling peripheral devices. Generally, central devices run software created specifically for interacting with these peripheral devices.

Peripheral devices act as sensors, which collect data and send the data to the central devices to be processed. This is key to BLE peripherals' low power use; they don't process data—they only collect and transmit it. The app is responsible for setting any options on the device and controlling the user's authentication process. To do so, it typically connects to a server in the cloud, which stores the person's account information. In some cases, the app also acts as an intermediary between various users seeking to use features like chat, videoconferencing, file transfers, or if device owners want to give control of their devices to remote users.

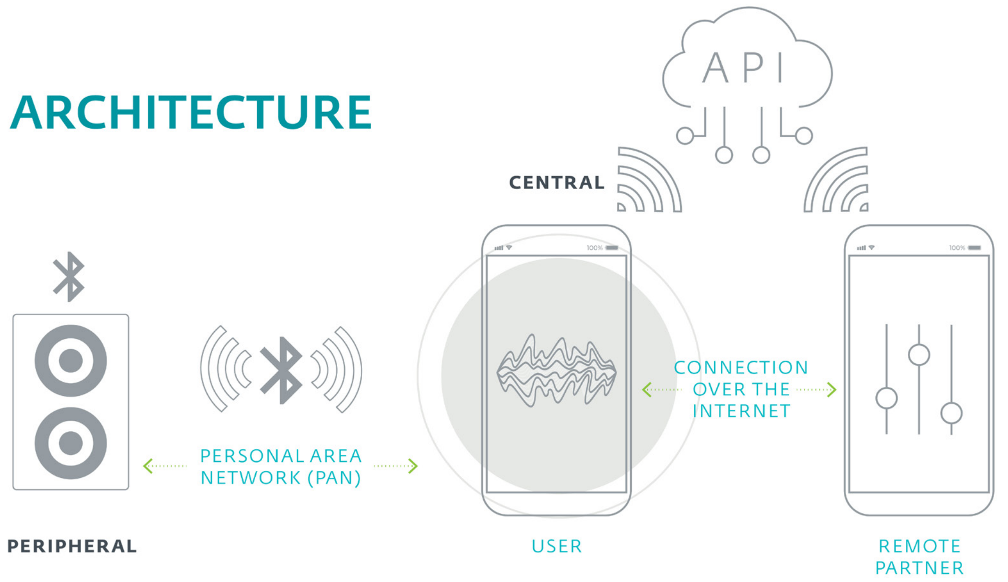


Figure 1 // Architecture of a smart sex toy

This architecture presents serveral weak spots that could be used to compromise the security of the data being processed: Intercepting the local communication between the controlling app and the device, between the app and the cloud, between the remote phone and the cloud, or directly attacking the cloud-based service. Of course, not all attacks take place over network connections, and some malicious scenarios could be launched using malware previously installed on the phone or by exploiting bugs in the phone's operating system. However, in this white paper we look only at vulnerabilities present in the app itself.

Despite the fact they have already been subjected to the scrutiny of many security researchers ([1], [2], [3], [4], among others), our investigation demonstrated that these devices continue to contain security flaws that could threaten the security of the data stored as well as the user's privacy and even safety. These vulnerabilities range from poor authentication procedures to devices that constantly publicize their presence, allowing anyone to connect to them.

WHY IS SECURITY SO CRITICAL WHEN IT COMES TO SEX TOYS?

It won't be news to anyone that IoT devices have vulnerabilities. In past articles, ESET has analyzed serious flaws found in multiple smart home hubs and *smart cameras*. Recently, *ESET researchers uncovered KrØØk*, a serious vulnerability that affected encryption of more than a billion Wi-Fi devices. However, with sex toys, the sensitivity of the information processed is extremely critical: Names, sexual or gender orientation, lists of sexual partners, information about device usage, intimate photos and videos—all these pieces of information can have disastrous consequences if they fall into the wrong hands.

Who could be interested in this type of information? In places such as *Alabama* in the USA, the sale of sex devices is illegal, although some models can still be found being advertised under medical euphemisms—as used to happen back in the year 1906 as Maines found in her research. Moreover, many deeply conservative countries have strict laws prohibiting some or all forms of homosexual, premarital, and extramarital sexual activity. In such countries, *primarily in Africa and Asia*, the publication of private information about individuals' sexual behavior and their partners could lead to their arrest, followed by jail, and possibly even a death sentence.

Under these circumstances, what would happen if a country or region's authorities launched an oppressive campaign based on the forceful expropriation of data from the companies that process them, or the exploitation of bugs or weaknesses in sex devices, as a way to identify, locate, and persecute homosexuals, adulterers, or anyone else belonging to a minority or social group, on grounds of their sexual choices?

In addition to concerns about government espionage, smart sex toys are not exempt from the possibility of being compromised by cyberattackers either. New forms of sextortion appear on the radar if we consider the intimate material accessible through the apps that control these devices.

There are already precedents, and they help us to get a sense of the scale of the possible consequences. The *attack on the Ashley Madison "dating site"* is perhaps the first example that comes to mind. After the names of more than 30 million users of the platform for "cheats" were published, countless *reports* of divorces, suicides and scams based on the leaked data appeared in the media.

As well as concerns about data confidentiality, we have to consider the possibility that vulnerabilities in a sex toy's controlling app could allow malware to be installed on the phone, or firmware to be changed in the toys. These situations could lead to DoS (Denial of Service) attacks that block any commands from being delivered, or a device that is weaponized in order to carry out malicious actions and propagate malware, or even a device deliberately modified to cause physical harm to the user, such as by overheating.

Alongside this, we cannot talk about the implications of an attack on a sexual device without also reassessing the significance of sexual abuse in the context of the digital transformation that society is going through. What are the consequences of someone being able to take control of a sexual device without consent, while it is being used, and send different commands to the device? Does current legislation allow the possibility to punish such behavior? Could that be described as an act of sexual assault?

The notion of cybercrime takes on a different appearance if we look at it from the perspective of invasion of privacy, abuse of power, and lack of consent for a sex act – some of these devices are wearable and a vulnerability might allow anyone within range to start operating them. Although most countries today have a legal framework that categorizes various types of cybercrime, we have not yet reached the point where we are evaluating new forms of abuse stemming from digital systems that, little by little, are being incorporated into the private lives of a great many users.

One thing is clear, though: Consent obtained through fraud is no consent at all, and this legislative gap in current laws will need to be resolved in order to ensure the sexual, physical, and psychological safety of users in the digital arena.

SECURITY EVALUATION OF TWO POPULAR DEVICES

The purpose of our research was to determine the level of security in Android apps created to control the most popular models sold by the main brands of sexual pleasure devices, in order to establish to what extent they ensure the confidentiality of their users' data.

One of the difficulties that arises when analyzing sexual devices—and IoT devices in general—is the wide variety of models available in the market, each with their own firmware and apps for controlling them. For this reason, we decided to limit our analysis to two of the best-known manufacturers in the international market, obtaining one of each of the following products: Max by *Lovense* and *We-Vibe* Jive.

First of all, we downloaded the vendor apps available on the Google Play Store for controlling these sex toys (*We-Connect* and *Lovense Remote*), and we used vulnerability analysis frameworks as well as manual analysis techniques to identify flaws in their implementations.

Device	App Name	App packet	Version	Hash
Jive	We-Connect	com.standardinnovation.weconnect	3.0.3	FC7780F593263975E11391000229EC51C831CEEC
			4.3.1	0E9F9E72E8BC0C392A285C6F5FDF33D21267DFC1
			4.4.1	E35006AA28B4539758BD72FCD8715E7516906F75
Max	Lovense Remote	com.lovense.wear	3.4.6	B7A8735C9F16252E564F841ECC9861C43F0B1D68
			3.5.8	A0CBBC09997038D8658B4E3BD644B7357A32123E
			3.7.1	E167CA3972ADB00D7B0141CFD7D2B8687139AD0E
			3.8.1	852E87FCBF774117342407A3E5D48C7AB7F38EBE
			3.8.4	8280097D01DFFC2AC75B1EC945CB77E868EC0DB9
			3.8.6	954D7562C75D71CDE30A73BEA5A0884C510CE0A1

Table 1 // Details of the apps that were analyzed

The following sections detail some of the security issues we found for each app and device. Both developers were sent a detailed report of the vulnerabilities and suggestions of how to fix them.

At the time of publication of this article, all vulnerabilities have been addressed.

We-Vibe

One of the best-known brands in the sex toy market is We-Vibe. A wide range of products is sold under this brand, including some smart devices. One interesting aspect of these devices is that a lot of them are designed to be used as wearables, and can actually be worn all day long. It was precisely for this reason that we chose to buy the Jive for our research, presuming wearable devices are prone to be used in environments that are inherently insecure.

Figure 2// The We-Vibe Jive

When we started our preliminary research, we discovered articles that had already been published that talked about major vulnerabilities discovered in the device. One article particularly worth mentioning is a discussion titled *Breaking the Internet of Vibrating Things*, which provides details of serious flaws found in the We-Connect app, which is used for all of the manufacturer's smart models. Specifically, the collection of sensitive information without user authorization led to a series of lawsuits against Standard Innovation (now part of WOW Tech Group) and the subsequent *payout of almost US$3.7 million* in 2017.

Following the settlement, the company decided to make changes to the app in order to remove any trace of personal information from its systems. Currently, the app does not store users' personal data, although its privacy policy does state that a token will be used in conjunction with the device's IP address in order to identify the device. Furthermore, data such as the language, model, operating system version, time, date, and unique ID of the phone are all collected, and the user is offered the option to share extra information about their use of the device by switching this feature on in the app's settings.

Another improvement made to the app within the last few years was the inclusion of certificate pinning, which means the app checks that the server it's connecting to is legitimate. Using this client-side validation technique, at runtime the app compares the server certificate against a list of trusted certificates embedded in the app itself. If they don't match, then the connection is terminated.

Although this increases the security for end users, it's easy to bypass the certificate pinning for study purposes by modifying the code of the APK to include a self-signed certificate or injecting the app with reverse engineering tools like *Frida*.

Bluetooth connection

Like many IoT devices, the Jive uses BLE to connect to and communicate with the user's mobile device. The main security features incorporated into BLE are 128-bit encryption and authentication. Communication via BLE is secure on devices that have already verified a connection. However, to connect, devices first have to pair with each other, and that is where the main weakness of the BLE system lies. To learn in detail how this protocol works in detail, you can visit *our article on BLE in WeLiveSecurity*.

During the first stage of pairing, the Jive and the mobile device exchange basic information about their capabilities in order to discover how to proceed with the connection. In other words, they identify themselves on the network, explain what they are (type of device, brand, model, etc.), and what they can do. This exchange is not encrypted.

The second stage of pairing involves generating and exchanging keys. This is the point where BLE connections can be manipulated: If the connection is not adequately secured, attackers can take control of the devices and of the data they send.

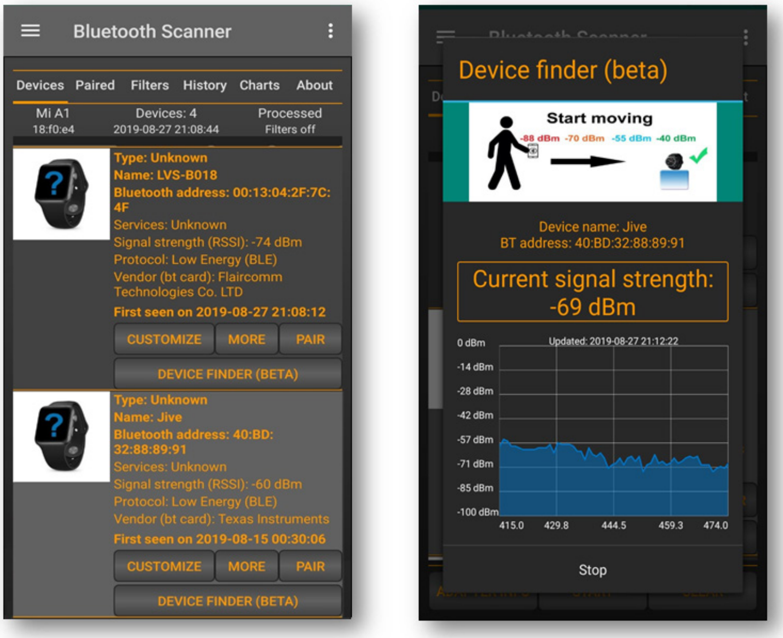
Lastly, bonding is the process during which the devices store the authentication data they exchanged during the initial pairing, which allows them to remember each other as being secured when they connect again in the future.

There are methods to make the second stage secure, such as using temporary keys to authorize the connection, or using BLE Secure, which is included in BLE version 4.2 and applies the Diffie-Hellman algorithm to generate keys, as well as incorporating a more complex authentication process. However, the Jive does not implement these methods, which makes it particularly vulnerable to man-in-the-middle (MitM) attacks.

In addition, since the Jive needs to be continually announcing its connection so the user can connect to it, anyone can use a simple Bluetooth scanner to find any such devices in their vicinity. In fact, this is what researcher Alex Lomas did, *walking the streets of Berlin with a smartphone discovering sex toys*, which announced their presence through Bluetooth connection notifications. This just goes to show that even in your own home, there is the possibility of someone unexpected intruding into the device.

In the case of our Jive device, these risks are increased due to the fact that it's a wearable, designed for the user to be able to wear it as they go about their day—at restaurants, parties, hotels, or in any other public location. In these situations, an attacker could identify the device and use the device's signal strength as a compass to guide them and gradually get closer until they find the exact person wearing it.

Figure 3 contains screen captures of a Bluetooth scanner that has found both the Jive and the Lovense Max (the device we will analyze in the next section, appearing here as "LVS-B018"). In one image, we see that the Jive announces itself with its model name, making it very easy to identify. The other image shows a signal strength of -69dBm, as the scanner approaches the device, this power level will increase, allowing its exact location to be found.



Type: Unknown
Name: LVS-B018
Bluetooth address: 00:13:04:2F:7C:4F
Services: Unknown
Signal strength (RSSI): -74 dBm
Protocol: Low Energy (BLE)
Vendor (bt card): Flaircomm Technologies Co. LTD
First seen on 2019-08-27 21:08:12

Type: Unknown
Name: Jive
Bluetooth address: 40:BD:32:88:89:91
Services: Unknown
Signal strength (RSSI): -60 dBm
Protocol: Low Energy (BLE)
Vendor (bt card): Texas Instruments
First seen on 2019-08-15 00:30:06

Device name: Jive
BT address: 40:BD:32:88:89:91

Current signal strength: -69 dBm

Figure 3// Discovery of sex toys available in the immediate vicinity, through a Bluetooth scanner

Once the Jive is connected to the user's mobile device, it will stop advertising, but when the app is closed, the connection drops and the toy starts to advertise itself again. With this in mind, there are "jammer" antennas available that can be used to block Bluetooth signals, and these can also be used by attackers to disconnect a peripherial device so that when the victimized device tries to reconnect, it will do so to a device controlled by the attacker, which allows taking control of the victim's device as well. In any of these ways, the Jive can become connected to a malicious device in the immediate surrounding area when the legitimate user's device is not connected to it.

Once an available Jive is found, an attacker does not even need to install the manufacturer's official app, as the Web Bluetooth feature included in most current browsers allows them to connect to and interact with the Jive (and other models) through existing websites that facilitate interacting with such sex toys. Serious privacy concerns were what led Apple to *decline the implementation of this Bluetooth Web API in Safari*.

BLE MitM

A BLE man-in-the-middle attack involves a malicious device that claims to be both central and peripheral at the same time, and tricks other devices on the network into connecting to it. In this case, not only can the attacker – within 6 to 8 meters (~19 to 26 feet) – eavesdrop the traffic from connected devices, but it would also be possible to send maliciously crafted packets to potentially exploit vulnerabilities. The best way to avoid this kind of attack is by using a secure, appropriate pairing method.

With the Jive, the device is paired using the "just works" method, which is the least secure of them all (and is unfortunately the one most IoT devices are preconfigured to use). With this method, the temporary key used by the devices during the second stage of pairing is set to 0, and the devices then generate the value of the short-term key on this basis. This method is highly vulnerable to MitM attacks, as any device can connect using 0 as the temporary key. In practical terms, this means any unpaired Jive will bond automatically with any mobile phone, tablet, or computer that requests it to do so, without carrying out any verification or authentication.

This is not the only problem: When the Jive is not paired to the app, it is constantly announcing its presence and waiting for a connection. That means attackers can easily take control of the device if they are within 9 meters of it.

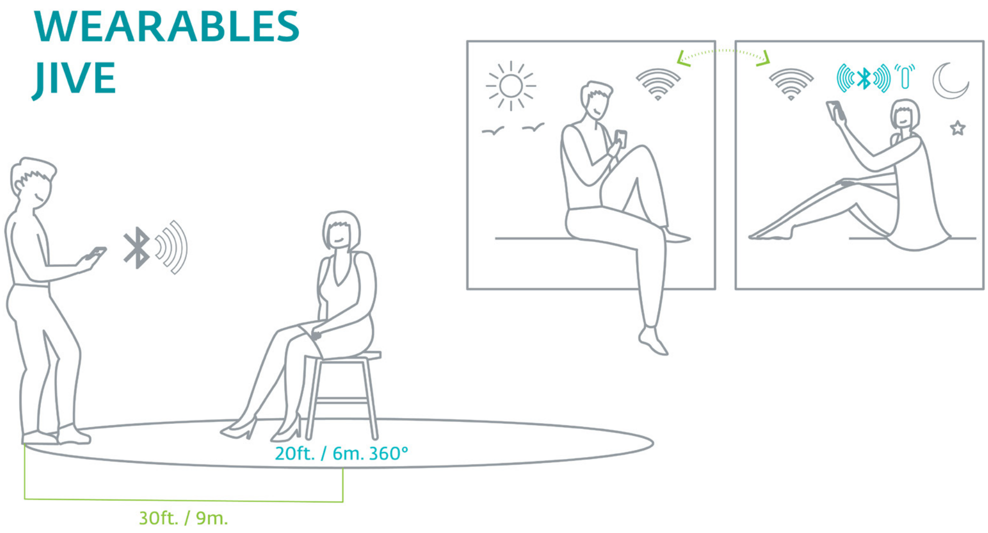


Figure 4// The Jive is a wearable device

In our proof of concept, we used the *BtleJuice* framework and two BLE dongles to replicate a man-in-the-middle attack between a user and the Jive. You can see a demonstration of this in the following video:

https://youtu.be/1o-qEOau1hg

In it, we simulated a scenario where an attacker first takes control of a Jive (which they connect to directly due to its lack of authentication) and then announces a dummy Jive device, which is set up based on the information that the original Jive announced. Next, when the user decides to connect to the toy, what they actually connect to is the fake device advertised by the attacker.

The attacker is then able, via the BtleJuice web interface, to capture all of the packets sent by the user and intended for the toy and thereby obtain information about the modes of use, intensity of vibration, etc. If they want, they can also edit the commands they intercept, changing the vibration mode or intensity. Lastly, they can generate their own commands and send them to the toy, even if the user is not interacting with it.

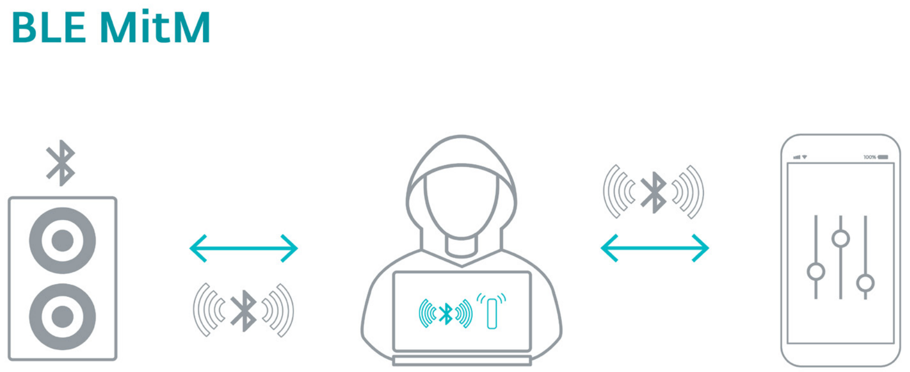
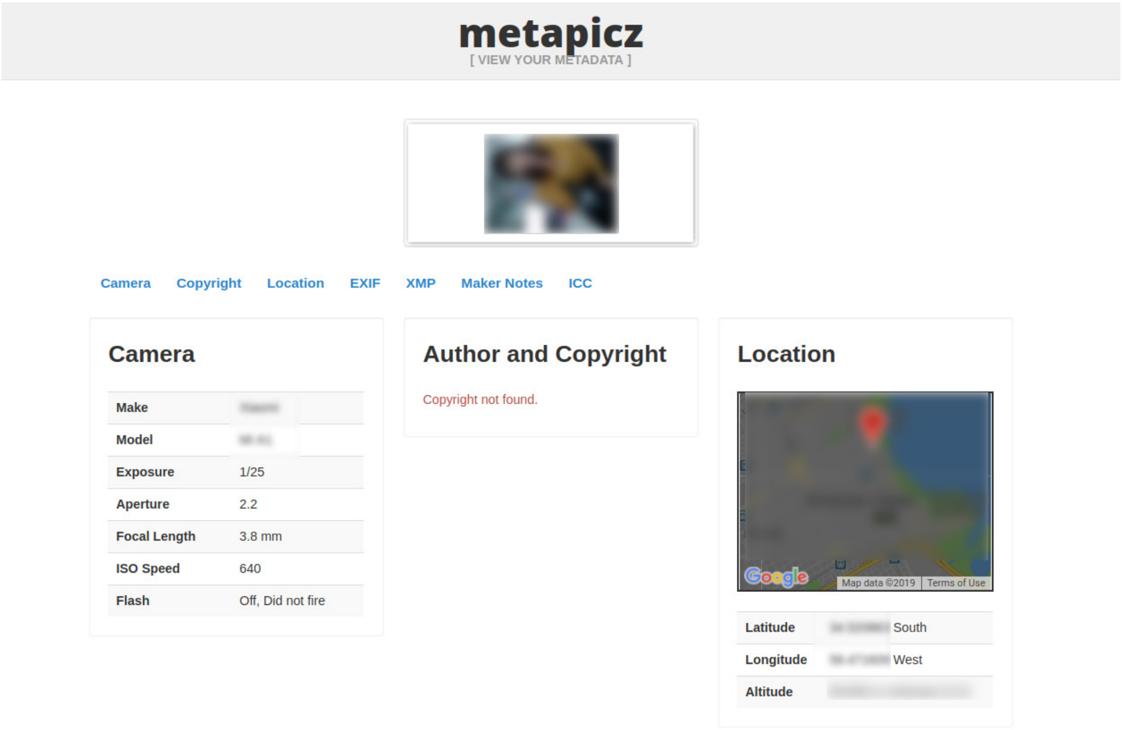


Figure 5// Architecture of a MitM attack taking place between a Bluetooth device and the app used to control it

Metadata

When we analyzed what happened to multimedia files shared between We-Connect users during chat sessions, we discovered that they are saved in the app's private storage folders – so they can't be accessed by other apps installed on the device – and are deleted immediately when the chat ends which, from a privacy perspective is a Good Thing. However, when we investigated what happened to the files' metadata, we were surprised to find that it was still on the shared file. This means that every time users send a photo to a remote phone, they may also be sending information about their devices and their exact geolocation.

Storing unprotected sensitive information on the device is never a good idea from a development standpoint, even when using the apps' private folders for this purpose. In this scenario, a malicious user with a rooted phone could access these files, analyze them using a website like metapicz, and obtain information about the users who originally shared the images, including GPS location and the smartphone model.



Camera

Make	[redacted]
Model	[redacted]
Exposure	1/25
Aperture	2.2
Focal Length	3.8 mm
ISO Speed	640
Flash	Off, Did not fire

Author and Copyright

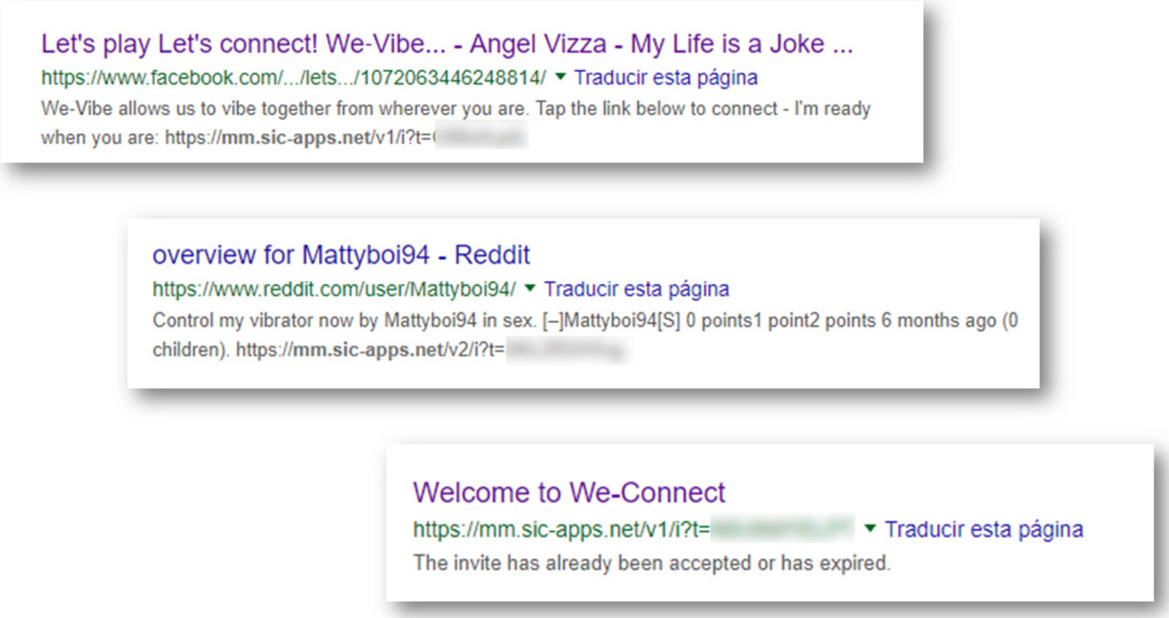
Copyright not found.

Location

Latitude	[redacted] South
Longitude	[redacted] West
Altitude	[redacted]

Figure 6// Metadata of images sent via the We-Vibe app's chat feature

This is hugely relevant because many Jive users intentionally hand over control of their device to complete strangers by publicly sharing its access URL online. In doing so, they may be inadvertently sharing more information than they think.



Let's play Let's connect! We-Vibe... - Angel Vizza - My Life is a Joke ...
https://www.facebook.com/.../lets.../1072063446248814/ ▾ Traducir esta página
We-Vibe allows us to vibe together from wherever you are. Tap the link below to connect - I'm ready when you are: https://mm.sic-apps.net/v1/i?t=[redacted]

overview for Mattyboi94 - Reddit
https://www.reddit.com/user/Mattyboi94/ ▾ Traducir esta página
Control my vibrator now by Mattyboi94 in sex. [–]Mattyboi94[S] 0 points1 point2 points 6 months ago (0 children). https://mm.sic-apps.net/v2/i?t=[redacted]

Welcome to We-Connect
https://mm.sic-apps.net/v1/i?t=[redacted] ▾ Traducir esta página
The invite has already been accepted or has expired.

Figure 7// Users sharing their tokens publicly

Lock PIN

The app gives its users the option to set a four-digit PIN to access it, but does not enforce any delay after a certain number of incorrect attempts, so it wouldn't take long for an attacker – who has physical access to the device – to find the correct PIN with brute force by using a *bad USB*. Since the number of possibilities is relatively low, an attacker could try all possible combinations and get the PIN in under 12 hours. You can watch a demonstration of this in the following video:

https://www.youtube.com/watch?v=8eYSUoyS9jw

Solutions to this problem could be to require a more complex password, add fixed or exponentially increasing delay intervals for PIN reentry after a certain number of incorrect attempts, and/or modify the GUI to include a grid of buttons instead of a keyboard input.

Lovense

The second device we analyzed was the Max Masturbator by Lovense. The interesting thing about this device is its ability to synchronize with a remote counterpart, which can be various other Lovense sex toys. The synchronization allows the device to replicate the movements of its remote counterpart. This scenario is interesting from a hacking perspective, as the attacker could take control of both devices by compromising just one of them.

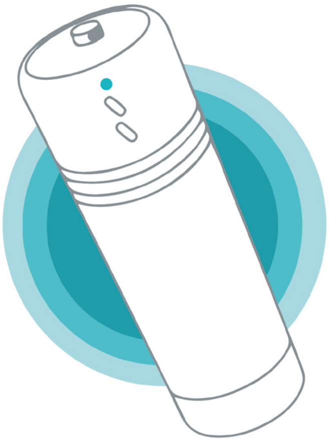


Figure 8// The Lovense Max

Privacy issues

Insecure design

The first thing that caught our attention in the Lovense Remote app were some controversial design choices that, in our opinion, may threaten the confidentiality of intimate images one user shares with another. The most significant of these is the option to forward images, which allows the recipient to further share that material with third parties but without requesting consent from, or even sending a notification to, the creator of the content.

The app also lets users download any multimedia content they receive, again without notifying the user who shared the content in the first place. This feature allows images received by the app to be stored on that phone's shared file system, where they can be accessed by other apps installed on the phone (including malware). For example, they could show up on Google Photos and even be backed up to the cloud through third-party services.

Although the chat feature includes the option to delete a message, it only hides the message on the local chat interface and does not delete it from the remote phone. This could lead to misunderstandings, with the sender thinking images previously shared have now been deleted from the recipient's phone and are safe, when in reality this is not the case.

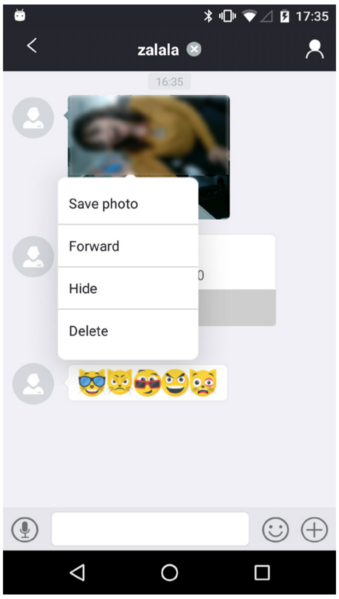


Figure 9// Options menu for multimedia files on Lovense Remote

In fact, even if you delete or block a user, that person will continue to have access to the chat history and all of the shared multimedia files. In the latest versions of the app there's an option to recall a message, which erases the content from the remote phone, but that option is only available for two minutes after sending a picture and then completely dissapears. Furthermore, the screen capture feature remains enabled, allowing a malicious user to take screenshots of anything in the chat.

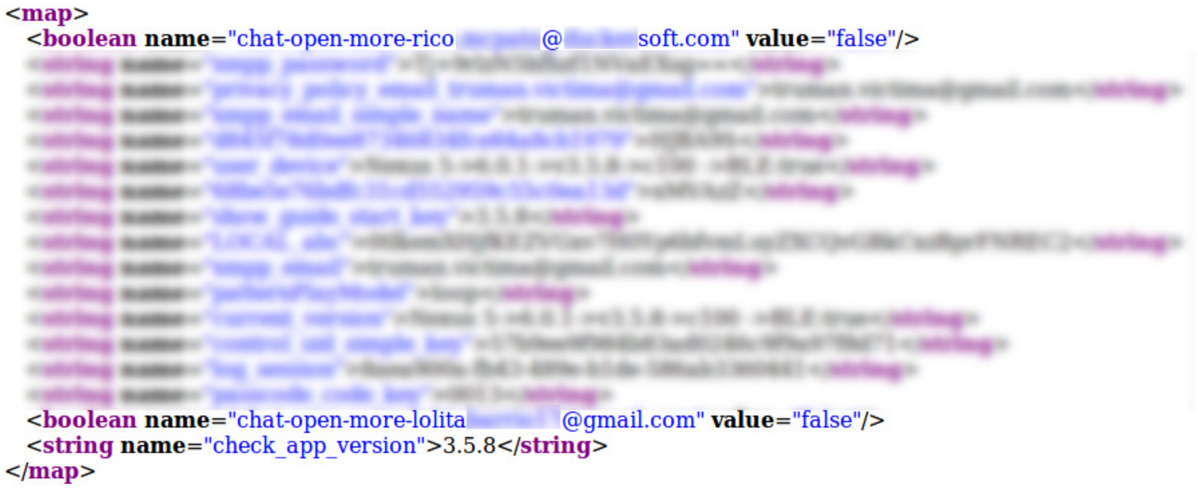
Pictures sent to the remote device solely rely on HTTPS for protection, there's no end-to-end encryption, and when stored on the server their secrecy depends on the secrecy of their file names, which are random IDs generated by the server at the time of upload. These pictures remain on the server for at least seven days, although most of them remain there much longer. Ultimately, once users have shared a piece of content, they lose all control of it.

Despite the fact that these are not vulnerabilities per se, these findings constitute serious privacy concerns. Nowadays, most IM apps allow users to delete messages any time they want or to set timers for message deletion. They let you know if the content you are receiving has been forwarded; they apply end-to-end encryption. If you're using a secret chat on Telegram, you can't take screenshots. As everyday IM apps become more secure, one would expect the same from apps specifically designed to share sexual content.

Information disclosure

Despite the fact that users typically present themselves to each other using fantasy names, the Lovense Remote app uses the email address users log in with as their IDs in the message-sending process. Not only that, but each email address is shared among all the phones involved in each chat, and is stored in plaint text in many locations, such as the shared preferences file wear_share_data.xml.

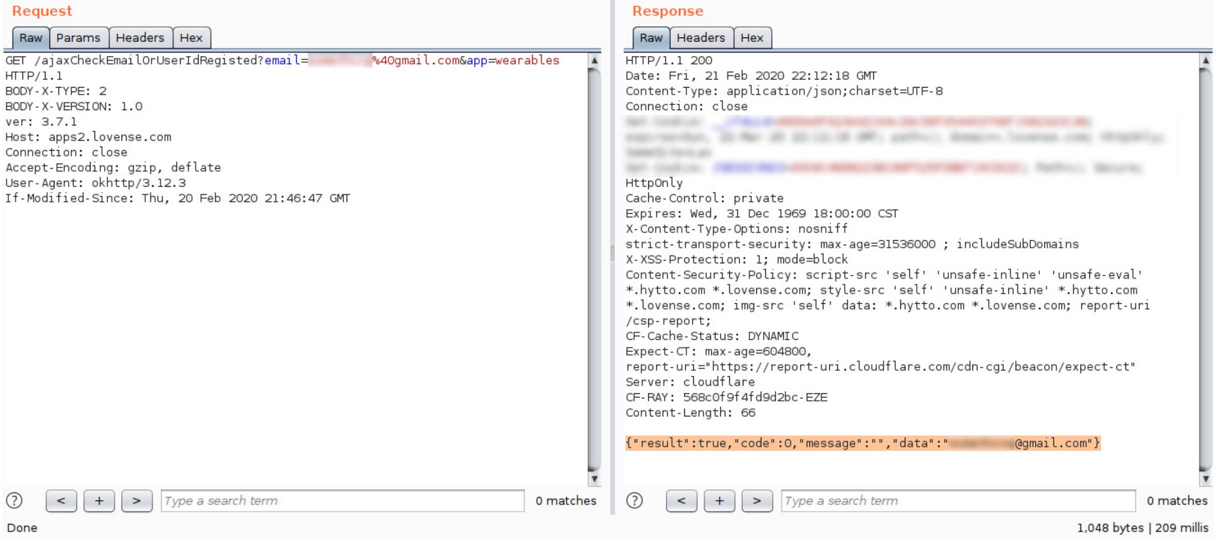
This means a malicious user could access the list of email addresses of users they have added as contacts. The attacker could then use this information to begin a process of identifying and recognizing users without their consent—by collecting information about them that is available online—to serve as a launchpad for subsequent attacks through social engineering, possibly involving sextortion.



```
<map>
  <boolean name="chat-open-more-rico[redacted]@[redacted]soft.com" value="false"/>
  [redacted]
  <boolean name="chat-open-more-lolita[redacted]@gmail.com" value="false"/>
  <string name="check_app_version">3.5.8</string>
</map>
```

Figure 10// Shared preferences from the Lovense sexting app, where sensitive information is published about other users

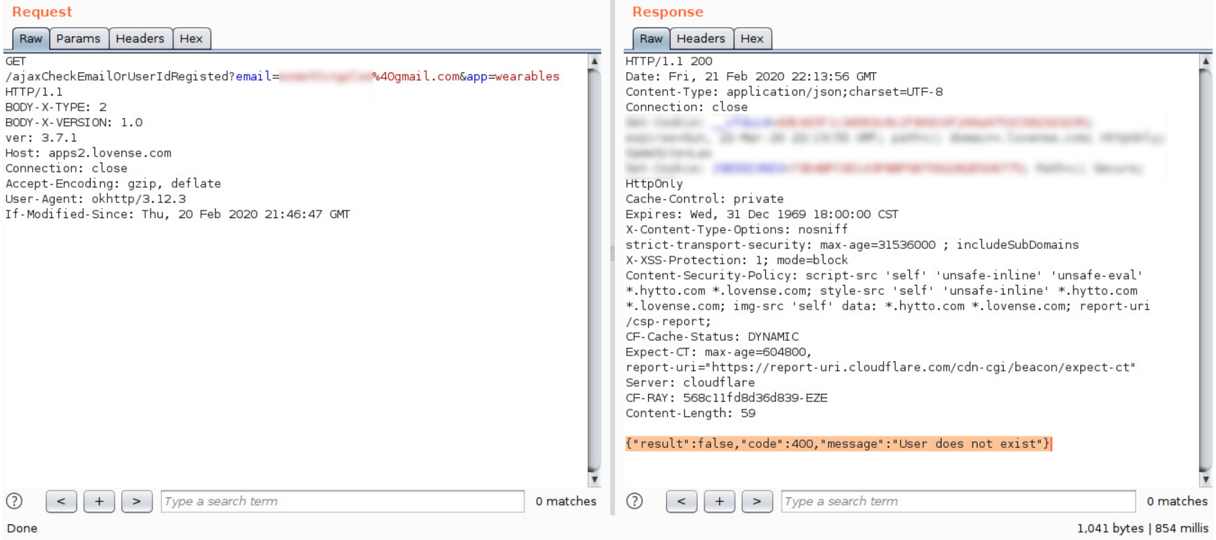
It is also possible to carry out the reverse process and find the user account associated with a particular email address if the email address is registered on the server. This is possible simply by sending a GET query to the server, indicating the email address you want to look up.



```
GET /ajaxCheckEmailOrUserIdRegisted?email=[redacted]%40gmail.com&app=wearables
HTTP/1.1
BODY-X-TYPE: 2
BODY-X-VERSION: 1.0
ver: 3.7.1
Host: apps2.lovense.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.3
If-Modified-Since: Thu, 20 Feb 2020 21:46:47 GMT
```

```
HTTP/1.1 200
Date: Fri, 21 Feb 2020 22:12:18 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
[redacted]
HttpOnly
Cache-Control: private
Expires: Wed, 31 Dec 1969 18:00:00 CST
X-Content-Type-Options: nosniff
strict-transport-security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval'
*.hytto.com *.lovense.com; style-src 'self' 'unsafe-inline' *.hytto.com
*.lovense.com; img-src 'self' data: *.hytto.com *.lovense.com; report-uri
/csp-report;
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 568c0f9f4fd9d2bc-EZE
Content-Length: 66

{"result":true,"code":0,"message":"","data":"[redacted]@gmail.com"}
```

Figure 11// This GET request queries whether the supplied email address matches a user account on the Lovense platform. In this case, the result is successful.



```
GET
/ajaxCheckEmailOrUserIdRegisted?email=[redacted]%40gmail.com&app=wearables
HTTP/1.1
BODY-X-TYPE: 2
BODY-X-VERSION: 1.0
ver: 3.7.1
Host: apps2.lovense.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.3
If-Modified-Since: Thu, 20 Feb 2020 21:46:47 GMT
```

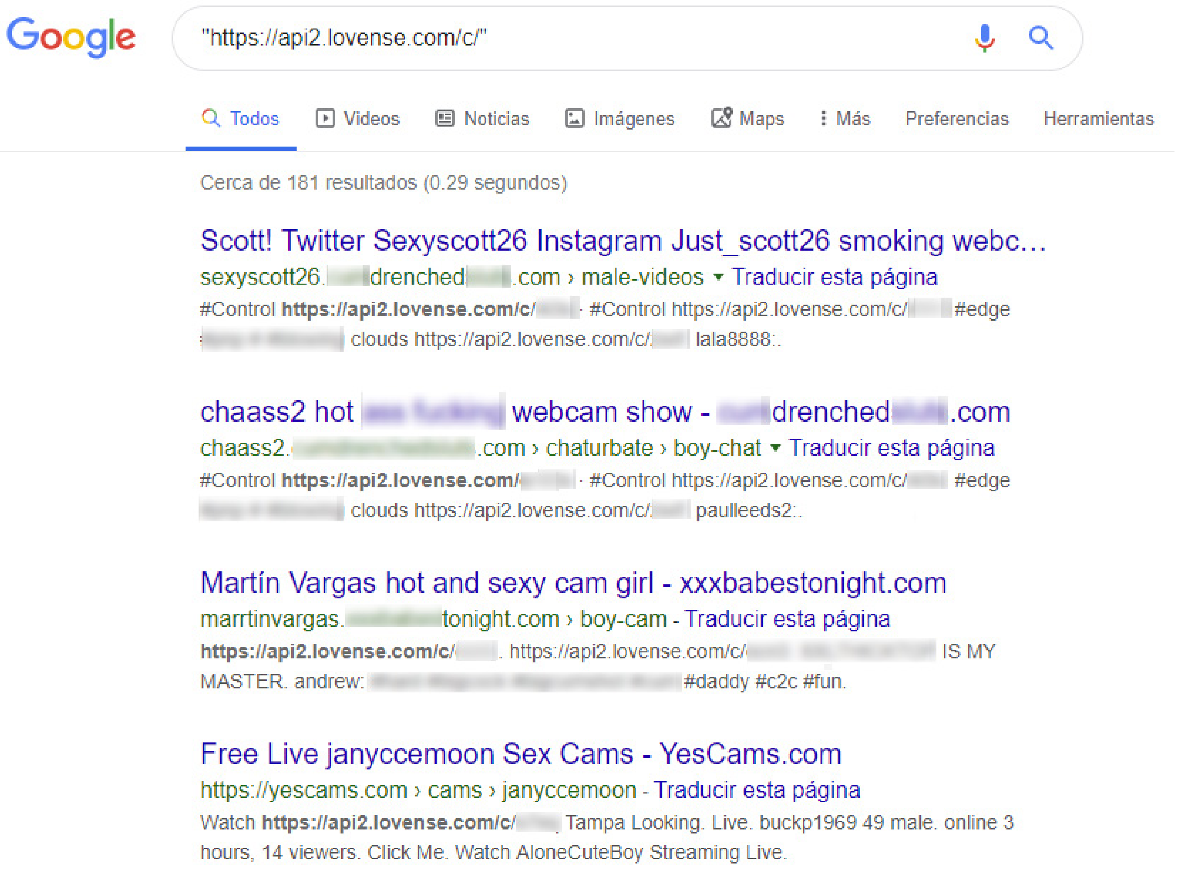
```
HTTP/1.1 200
Date: Fri, 21 Feb 2020 22:13:56 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
[redacted]
HttpOnly
Cache-Control: private
Expires: Wed, 31 Dec 1969 18:00:00 CST
X-Content-Type-Options: nosniff
strict-transport-security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval'
*.hytto.com *.lovense.com; style-src 'self' 'unsafe-inline' *.hytto.com
*.lovense.com; img-src 'self' data: *.hytto.com *.lovense.com; report-uri
/csp-report;
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 568c11fd8d36d839-EZE
Content-Length: 59

{"result":false,"code":400,"message":"User does not exist"}
```

Figure 12// In contrast to Figure 11, here the server returns a negative response to a query about an email address

Remote control through the brute forcing of tokens

The app's list of options for its remote control features includes not only the possibility to give control of the device to a user in your contact list, but also the option to generate a URL in the format `https ://api2.lovense.com/c/<TOKEN>`, where `<TOKEN>` is a combination of four alphanumeric characters. This allows remote users to control the device simply by entering the URL into their browsers.

Some users choose to share their tokens publicly, whether that's as personal choice or as part of a *camgirl* service. Communities on Reddit are the most popular option for sharing tokens anonymously. The use of email addresses as the users' IDs in the configuration files could be a threat to the privacy and physical safety of users who are not even aware of how much information they are really exposing.



Cerca de 181 resultados (0.29 segundos)

Scott! Twitter Sexyscott26 Instagram Just_scott26 smoking webc...
sexyscott26.[redacted]drenched[redacted].com › male-videos ▾ Traducir esta página
#Control **https://api2.lovense.com/c/**[redacted] · #Control https://api2.lovense.com/c/[redacted] #edge [redacted] clouds https://api2.lovense.com/c/[redacted] lala8888:.

chaass2 hot [redacted] webcam show - [redacted]drenched[redacted].com
chaass2.[redacted].com › chaturbate › boy-chat ▾ Traducir esta página
#Control **https://api2.lovense.com/**[redacted] · #Control https://api2.lovense.com/c/[redacted] #edge [redacted] clouds https://api2.lovense.com/c/[redacted] paulleeds2:.

Martín Vargas hot and sexy cam girl - xxxbabestonight.com
marrtinvargas.[redacted]tonight.com › boy-cam - Traducir esta página
https://api2.lovense.com/c/[redacted]. https://api2.lovense.com/c/[redacted] IS MY MASTER. andrew: [redacted] #daddy #c2c #fun.

Free Live janyccemoon Sex Cams - YesCams.com
https://yescams.com › cams › janyccemoon - Traducir esta página
Watch **https://api2.lovense.com/c/**[redacted]. Tampa Looking. Live. buckp1969 49 male. online 3 hours, 14 viewers. Click Me. Watch AloneCuteBoy Streaming Live.

Figure 13// Tokens allowing remote control of Lovense devices can be easily found via search engines or social networks

The app warns its users that the token is automatically deactivated after 30 minutes of inactivity or if the user generates a new code from the app. However, we were able to confirm that tokens remained active after the half hour was up. We were not able to determine a specific time frame before expiration nor the causes of this expiration, but some tokens remained active for days.

Surprisingly for such a short token with relatively few possible combinations (1,679,616 possible tokens on an app with over a millon downloads), the server does not have any protection against brute force attacks. As such, the question arises: Is it possible to use brute force to find tokens that are valid (i.e. have existed at some point in time) and active (i.e. have not yet expired and still allow remote control)?

To understand how tokens work, we used the Lovense Remote app, a few testing smartphones, a Lovense Max device and a desktop web browser. We created tokens in a controlled environment and studied the network traffic while accessing them via the browser and other phones.

When a query is made using a nonexistent token, the server redirects to `/redirect` and returns the JSON message `{"result":true,"code":404,"message":"Page Not Found"}`. However, if the token is valid, the server redirects to another URL in the format `https://[apps|api2].lovense.com/app/ws/play/<SID>`, which in turn redirects to `https://[apps|api2].lovense.com/app/ws2/play/<SID>`. Where `<SID>` is the session ID: an MD5-like string that unequivocally identifies the user and the ID of the device for which it was created. A token expires when its time limit is up (presumably), or when someone visits the final URL after going through the whole redirection process.

From this, we can deduce that it is possible to distinguish between valid tokens, active tokens, and expired tokens, depending on the response from the server. To check if this is true, first we listed dozens of tokens: we created some of them with our device, and then added other random tokens. Most of the tokens generated by our device had already expired, but one was still active. Then we programmed a simple Python script and we used it against this set of tokens. When this script finds a valid token, it opens the final URL in the browser and checks if the session has expired with the help of a Chrome extension we designed for the purpose of this research. If the session is found to be active, it sends a message through a Telegram bot to the specified account, notifying it of the new control panel found. We recorded a proof of concept video, available here:

https://youtu.be/5lWSaJC3WWU

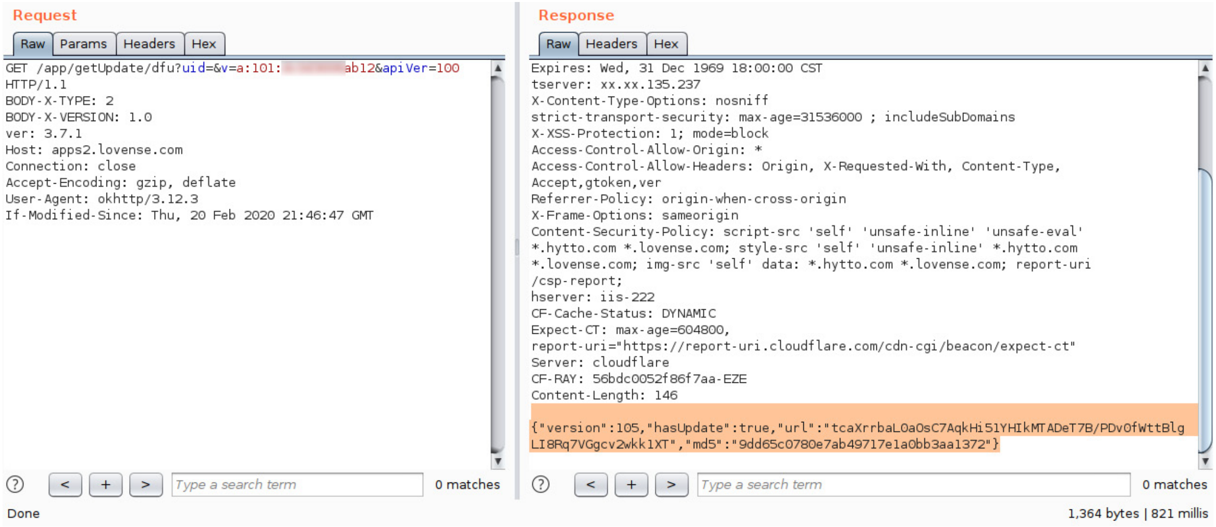
Working alongside the vendor, we were able to confirm that it was possible to find tokens from random users using brute force. This is an extremely serious vulnerability, as it allows an attacker to easily carry out remote hijacking of devices that are expecting connections through active tokens, without the user's consent or knowledge. Solutions to this flaw could include expanding the alphabet and increasing the length of the token to reduce the rate of correct guesses, invalidating the token immediately after the first redirect, eliminating the redirect process, and/or implementing mechanisms to protect the server from brute force attacks.

Bluetooth connections

Lovense Max device does not have authentication for its BLE connections either, so a MitM attack can be used to intercept its connections and send commands in the same way as explained above for the Jive. The commands to control the device's motors can easily be intercepted while sniffing the traffic between the device and the smartphone.

Firmware updates

When it comes to firmware updates, Lovense Remote also has some weaknesses. A firmware update process starts when the app sends a message to the server, asking if there are any updates available for the type of device, its ID, and the current version. If there are, the server responds with an encrypted URL, and the hash of the ZIP file to download.



```
GET /app/getUpdate/dfu?uid=&v=a:101:[redacted]ab12&apiVer=100
HTTP/1.1
BODY-X-TYPE: 2
BODY-X-VERSION: 1.0
ver: 3.7.1
Host: apps2.lovense.com
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.12.3
If-Modified-Since: Thu, 20 Feb 2020 21:46:47 GMT
```

```
Expires: Wed, 31 Dec 1969 18:00:00 CST
tserver: xx.xx.135.237
X-Content-Type-Options: nosniff
strict-transport-security: max-age=31536000 ; includeSubDomains
X-XSS-Protection: 1; mode=block
Access-Control-Allow-Origin: *
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type,
Accept,gtoken,ver
Referrer-Policy: origin-when-cross-origin
X-Frame-Options: sameorigin
Content-Security-Policy: script-src 'self' 'unsafe-inline' 'unsafe-eval'
*.hytto.com *.lovense.com; style-src 'self' 'unsafe-inline' *.hytto.com
*.lovense.com; img-src 'self' data: *.hytto.com *.lovense.com; report-uri
/csp-report;
hserver: iis-222
CF-Cache-Status: DYNAMIC
Expect-CT: max-age=604800,
report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 56bdc0052f86f7aa-EZE
Content-Length: 146

{"version":105,"hasUpdate":true,"url":"tcaXrrbaL0a0sC7AqkHi51YHIkMTADeT7B/PDv0fWttBlg
LI8Rq7VGgcv2wkk1XT","md5":"9dd65c0780e7ab49717e1a0bb3aa1372"}
```

Figure 14// Query to start a firmware update

However, due to the lack of use of *certificate pinning*, and as the decryption keys are stored within the app's code, it is relatively simple for an attacker to create a script to intercept the packets and redirect the victim to the attacker's malicious URL.

BEST PRACTICES TO AVOID THESE RISKS

The use of sex toys that are remotely controlled via apps is gaining popularity as part of the concept of "sexnology": A combination of sex and technology. These practices may well be here to stay, but we must not forget the potential threats to users' privacy and intimacy.

To minimize the risks associated with the use of smart sex devices, we recommend keeping in mind the following advice on privacy and sexting:

- Some apps offer the possibility to control devices locally via BLE without creating a user account. If you are not planning on letting other users control your device remotely over the internet, look for one of these apps.
- As much as possible, avoid sharing photos or videos in which you can be identified, and do not post remote control tokens on the internet.
- Avoid registering for sex apps using an official name or email address that could identify you—in other words, try to be as anonymous as possible. Consider creating a new email account exclusively dedicated to these apps.
- Always read the terms and conditions of apps and websites for which you register or to which you send any information. Pay special attention to the sections that talk about data collected by the company as well as the processing of that data. Vendors without a privacy policy should be avoided.
- Revisit these policies frequently to check for updates. Visit the manufacturer's web site periodically to look for changes that might not have been announced via the application.
- Use smart sex toys in a protected environment and avoid using them in public places or areas with people passing through (like hotels).
- When using the toy, keep the app connected to it, as this prevents the toy from advertising its presence.
- Turn off the device and disable Bluetooth when not in use.
- Download the control apps and try out their features before buying the device to get an overview of how secure the app is. Another recommendation is to use search engines to find out if the model you are thinking of buying has had serious vulnerabilities in the past, if there are security patches for it, and if there are frequent updates from the developer. Sending an email to the customer support department may clarify any doubts you have in this respect.
- Always protect the mobile devices you use to control these gadgets, keep them updated, and have a security solution installed on them.
- Protect the home Wi-Fi network you use for the connection with strong passwords, secure encryption algorithms, and regular updating of the router's firmware.

Lastly, if you believe or know that the device you already own has serious vulnerabilities, we strongly recommend that you avoid using its remote control features. As far as possible, disable the Bluetooth or remote connections while it is not in use.

FUTURE RESEARCH

As you will have noticed, for this analysis we looked at only Android apps, so it remains to be seen how vulnerable the apps for iOS devices are. Furthermore, there is a very wide variety of models available and for obvious reasons we have not been able to analyze all of their firmware and their intercommunication with the apps associated with them. Going forward, we would like to obtain new devices from other brands to carry out a second set of research in this area. The study of device firmware itself, through the use of fuzzing techniques, is another aspect that has not yet been fully developed.

On the other hand, dating and hookup apps could be considered as one of the earliest developments on the road to the normalization of digitalized sex, but that road has not been entirely free of obstacles. Tinder, for example, has had flaws that allowed people to *obtain a user's geographic location*, or *create fake profiles to connect with other people* without their consent. As the volume of users has increased, *scams* have become commonplace on these platforms. Meanwhile, new apps have emerged over the course of time and today there is a wide range of them to choose from. A systematic analysis of dating and hookup apps and their vulnerabilities, in order to establish how secure they are nowadays, would make a good addition to this research into the level of security of sex on digital media.

And finally, many advances have been made in the design and creation of sex robots. Some models include cameras, microphones, as well as voice analysis capabilities based on machine learning techniques. Being aware of *known vulnerabilities in robot environments*, we contacted sex robot manufacturers asking them for information about their security features, and the results were not at all encouraging. A lot of these robots are based on Android phones, which manage their sensors just as they would manage peripheral devices, and add machine learning capabilities through apps. These apps are not made available through official stores, so updates are sent to users by email, which creates major security holes. The *use of robots as replacements for sex workers in brothels* is already a reality, so a study of their limitations in terms of information security is essential in order to boost the development of security in these new technologies.

ACKNOWLEDGEMENTS

We would like to thank WOW Tech Group and Lovense for their good cooperation on dealing with the reported issues.

We are publishing the vendors' official statements regarding our disclosure:

WOW Tech Group:

Given the intimate nature of our products, the privacy and security of our customers' data is of utmost importance to WOW Tech Group. We take reports and findings by external sources about possible vulnerabilities very seriously. That is also why we are in close contact with ESET about the results of their research and are thankful for their work.

We had the opportunity to patch the vulnerabilities before the presentation and the publication of this report and have since updated the We-Connect App to fix the problems that are described in this report. In detail, we have added a timeout whenever a pin is entered incorrectly to reduce the risk of automized hacking attacks. We have updated the app to remove multimedia metadata before transmission and delete files at the end of each chat session – no metadata is stored or saved within the app or on our servers. These improvements were already tested by ESET and found to have removed the previous security issues.

Moreover, we conduct regular security audits and address security issues as they are discovered to comply with current best practices and security standards. With the help of external security and privacy experts, we strive to continuously strengthen our data protection and security measures to offer safe products to our customers.

Lovense:

Putting the health and safety of our users first, Lovense works tirelessly to improve the cybersecurity of its products and software solutions. Thanks to productive cooperation with ESET Research Lab, we were able to detect some vulnerabilities which have been successfully eliminated. Lovense will continue to cooperate with cybersecurity testers to ensure maximum security for all users of Lovense products.

TIMELINE OF DISCOVERIES

Q3 2019 – Started testing the Jive from We-Vibe and the Max Masturbator by Lovense.

We-Vibe Jive

Jun 19, 2020 – Emailed WOW Tech Group to report vulnerabilities.
Jun 24, 2020 – Emailed WOW Tech Group to report vulnerabilities.
Jul 22, 2020 – Emailed WOW Tech Group to report vulnerabilities.
Jul 22, 2020 – First response from WOW Tech Group.
Jul 24, 2020 – WOW Tech Group acknowledged the vulnerabilities.
Aug 3, 2020 – We-Connect version 4.4.1 released with fixes to the PIN locker and metadata issues.

Lovense Max

Jun 19, 2020 – Emailed Lovense to report vulnerabilities.
Jun 24, 2020 – Emailed Lovense Security Team to report vulnerabilities.
Jun 30, 2020 – Vulnerability report acknowledged by Lovense.
Jul 27, 2020 – All vulnerabilities discussed in this whitepaper were fixed in version 3.8.6 of the Lovense Remote app and made publicly available on the Google Play Store.
Oct 10, 2020 – Lovense continues to work on new privacy features for their app.

ABOUT ESET

For 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn *100 Virus Bulletin VB100* awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.