

Oclean Mobile Application decryptor

GPL-3.0 license  
0 stars 0 forks

Star

Notifications

<> Code Issues Pull requests Actions Projects Security Insights

main

Go to file

c3r34lk1l13r Add files via upload ... on Feb 11, 2021 4

[View code](#)

README.md

# decrypt-oclean-traffic

Oclean Mobile Application decryptor

Oclean Mobile Application 2.1.2 communicates with an external website using HTTP so it is possible to eavesdrop the network traffic. The content of HTTP payload is encrypted using XOR with a hardcoded key, which allows for the possibility to decode the traffic.

Decompiling the application you can find this code:

```
public static byte[] XOR(byte[] bArr) {
    char[] charArray = "#0+1C9L8E3A1%N00=2N7E".toCharArray();
    int length = charArray.length;
    for (int i = 0; i < bArr.length; i++) {
        bArr[i] = (byte) (bArr[i] ^ charArray[i % length]);
    }
    return bArr;
}
```

Following the cross-reference it is possible to see that is used for TX/RX datas to [OcleanAPI](#).

Timeline:

- 2020/09/01 Vulnerability found
- 2020/09/07 Contact with Oclean
- 2020/09/09 Oclean ack the vulnerability
- 2020/09/09 Contact Mitre for CVE
- 2021/02/11 CVE-2020-25493 Reserved

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%