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 = "#O+1C9L8E3A1%N0O=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 possibile 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