Security Advisory 2105-01

Security Advisories

Unencrypted cleartext transmission of sensitive information

Overview

Advisory ID: TRSA-2105-01
Advisory version: 1.0
Advisory status: Public
Advisory URL: https://trovent.io/security-advisory-2105-01
Affected product: VeryFitPro Android mobile application (com.veryfit2hr.second)
Tested versions: VeryFitPro 3.2.8
Vendor: Shenzhen DO Intelligent Technology Co., Ltd, http://www.i-doo.cn
Credits: Trovent Security GmbH, Nick Decker

Detailed description

Trovent Security GmbH discovered that the VeryFitPro mobile application performs all communication with the backend API via cleartext HTTP.
This includes login, registration and password change request. This allows an attacker in the same local network as well as all network devices between source and destination to steal sensitive information or even take control of user accounts.

Severity: High
CVSS Score: 7.5 (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)
CWE ID: CWE-319
CVE ID: CVE-2021-32612

Proof of concept

This is the TCP packet with the login request including password hash and username in cleartext:

```
$ host veryfitproapi.veryfitplus.com
veryfitproapi.veryfitplus.com has address 47.254.154.79
```

REQUEST:

```
12:07:13.267203 IP Kali.36786 > 47.254.154.79.http: Flags [P.], seq 1:304, ack 1, w
in 502, options [nop,nop,TS val 3095874488 ecr 477042156], length 303: HTTP: POST /
user/login HTTP/1.1
    0x0000:  4500 0163 6cb7 4000 4006 416b c0a8 007d  E..cl.@.@.Ak...}
    0x0010:  2ffe 9a4f 8fb2 0050 196c 8bba 4fc9 359b  /..O...P.l..O.5.
    0x0020:  8018 01f6 8cc8 0000 0101 080a b887 4bb8  ..............K.
    0x0030:  1c6f 15ec 504f 5354 202f 7573 6572 2f6c  .o..POST./user/l
    0x0040:  6f67 696e 2048 5454 502f 312e 310d 0a43  ogin.HTTP/1.1..C
    0x0050:  6f6e 7465 6e74 2d54 7970 653a 2061 7070  ontent-Type:.app
    0x0060:  6c69 6361 7469 6f6e 2f78 2d77 7777 2d66  lication/x-www-f
    0x0070:  6f72 6d2d 7572 6c65 6e63 6f64 6564 0d0a  orm-urlencoded..
    0x0080:  436f 6e74 656e 742d 4c65 6e67 7468 3a20  Content-Length:.
    0x0090:  3931 0d0a 486f 7374 3a20 7665 7279 6669  91..Host:.veryfi
    0x00a0:  7470 726f 6170 692e 7665 7279 6669 7470  tproapi.veryfitp
    0x00b0:  6c75 732e 636f 6d0d 0a43 6f6e 6e65 6374  lus.com..Connect
    0x00c0:  696f 6e3a 2063 6c6f 7365 0d0a 4163 6365  ion:.close..Acce
    0x00d0:  7074 2d45 6e63 6f64 696e 673a 2067 7a69  pt-Encoding:.gzi
    0x00e0:  702c 2064 6566 6c61 7465 0d0a 5573 6572  p,.deflate..User
    0x00f0:  2d41 6765 6e74 3a20 6f6b 6874 7470 2f33  -Agent:.okhttp/3
    0x0100:  2e38 2e30 0d0a 0d0a 6172 6561 3d45 7572  .8.0....area=Eur
    0x0110:  6f70 6526 7061 7373 776f 7264 3d64 3831  ope&password=d81
    0x0120:  3962 3832 3536 3665 3962 3630 3164 3837  9b82566e9b601d87
    0x0130:  6531 3638 6430 6466 6665 3331 6365 6531  e168d0dffe31cee1
    0x0140:  6139 3232 3926 6163 636f 756e 743d 6e2e  a9229&account=n.
    0x0150:  6465 636b 6572 2534 3074 726f 7665 6e74  decker%40trovent
    0x0160:  2e69 6f                                  .io
```

Solution / Workaround

To mitigate this vulnerability, we recommend to only use HTTPS when sending sensitive data from and to the application.

History

2021-05-02: Vulnerability found
2021-05-05: Advisory created
2021-05-12: CVE ID requested & vendor contacted
2021-05-14: CVE ID received
2021-05-25: No reply from vendor, contacted vendor again
2021-06-16: No reply from vendor, advisory published

ENGLISCH