

main [CVEs / CVE-2022-22908 /](#)



Err0r0x41414141 Update Readme.md ...

on Feb 26 [History](#)

..



Readme.md

9 months ago

[Readme.md](#)

## Coordinated Disclosure Timeline

04/01/2022: Report submission to Vendor via Ticket

05/01/2022: Vendor acknowledged CVE and has been notified of my intention to publish the advisory

05/01/2022: CVE submission sent to MITRE.org

17/02/2022: CVE reservation "CVE-2022-22908"

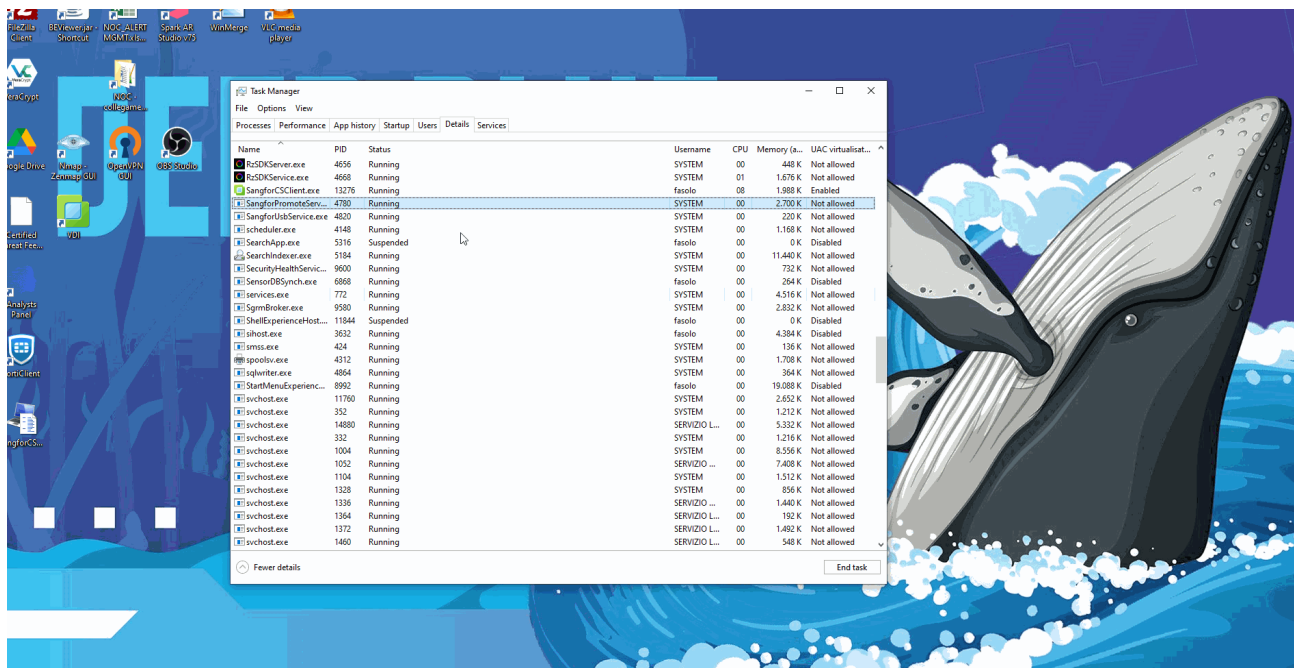
26/02/2022: CVE advisory publishment via this repository

## Executive Summary

An issue found in "SangforCSClient.exe", a core component of Sangfor VDI Client v5.4.2.1006 allows attackers to access user credentials via unspecified vectors.

## Technical Summary

To exploit the vulnerability an attacker must get a Full Dump of the "SangforCSClient.exe" process after the user inserted at least one time his credentials and clicked "Log In" button. After a Log In try any string previously inserted in "Username:" and "Password:" textboxes will be written in plaintext inside the Full Dump near known and standard strings or hex array.



IMPORTANT: this local vulnerability can expose useful information to an attacker willing to escalate his privileges. After a successful attack lateral movement can be done via multiple ways.

## Product

Sangfor VDI Client

## Tested Version

v5.4.2.1006

## Details

**Issue:** Sensitive data written in plaintext into process working memory

After dumping the process Memory you can look for the victim password near the following HEX sequence

Password location is near "based authentication" string, or seen in HEX:

```
62 61 73 65 64 20 61 75 74 68 65 6E 74 69 63 61 74 69 6F 6E
```

the username is usually inside the first part of the memory dump, just like you can see in the following screenshot

#### Testo decodificato

```
.....ø²...Æ>°wŮ°... ..PC<.Ž>°wŮ.1.{(±w±÷İÖ...ë.....³.....Øu³wP
C<.(±wQ÷İÖ...ë.....8³...ë...i@³.....°.....h³...C:\WINDOWS\SYSTEM
32\SangforSsleay32.dll.gdiplus_6595b64144ccfldf_1.1.19041.1<+°wE
ö°wŷŷŷŷ ±.....œ±.....°ö°w...ë.4...D³...°q±w{(±w%öİÖT³...°q±w{(±w°
öİÖ...ë.....8³.....{(±wıö.G...ë.%«°wö±...;Nv.°...°wA...Ä´...|°...
.....°´...°´...3°w´´.....Ä´...|°...°q...°µ...°ı...w°cŷŷ...x@.w(.ë...
.ë...æ...æ.....Ä´.....Ä´
.K...ä...Xp.....pŷŷŷÄ.ë....."....7|ŷŷ.....^....!.....
.....$.....ÈNç.....ë.....P.....æ.ŷ
.....æ...æ...°...ë.0.ä.Ä.ë.....p.ë.È.ä.....P
.ë...æ.Ä.ë.^°X(q...@.°w%«°wŷŷŷŷ1³...;Nv|³...°wA...@q...ø³.....
...°ö...q...3°w°ö.....@q...ø³...°ö...q...ı...w...ë...x@.w(.ë...ë...
P±wdu...°q±w{(±w@öİÖ...ë.....q.....@q...ıö.G"(J.f
..f....|q.....7...ıö.G\´.....<|ŷŷ....#|ŷŷ....f...€...°ŷä..
.ë.!...6|ŷŷ#.....°ŷä..°...ë.A...V|ŷŷeöİÖxWç.qı5ë.....!.....
.....).....#.....°...ä.ö.ë.....€...f...Ä.ë...ë.°h.wÄ´.....
.....Xp...°vã.Pu...b±w|... ..ŷŷŷŷ...ë.ŷŷŷŷ...ë.4Fë.....ë.....
...D.U.d...D.U.....#...ıë.xvã.....U.....U.Ä.U..
.....<.U.....ë.8.U.....ë.tu...B|±w...B|±w.....<¬ä....."
µ...€uŷv...ë.....ŷŷŷŷ....")I.8Ö...æ-troe÷O.°ö...")I.°µ.....TÖ...È
µ...œ÷O.Đp...|E.°Pæ.....q...4q...ô;E.°Pæ.ôwä.<¬ä.....q...°«.w °ŷä.Ä
q.....B|±w.q...±|E.....°Pæ.°Pæ.°Pæ.,q...°E.°Pæ.tq...<¬ä.Lq...~ E.°
Pæ.tq...°ö...°ö...")I.....\q...ÄžE.tq...<¬ä.lq...FšE.l¬ä...¬ä.Øö...éH@.x
Kä...pšë.....xKä.Øœë.....xKä.xKä.€Wç.€Wç.xKä.....È.|.....
...USERTEST...9A25EE63DD77ADAD7C3DF78E50D7F67ACF1CE9FF6A480A8E12C
1FC582564ABC5D725B8CF992FDB10A61B71414505B137B5DA63A9F1A3B288F18
996D528F76794ABC2071FF19CF5EE895830401200E7B616EEC509D7A5C3B79A7
8F802F43A8D71C671E58E2B8D12580920A667DC02ED8AC2038BEB87A47234800
171F8609F5C649FCDAD781BFCC832309B3750BEC54F856BC0C5B170850B20373
51C50505B2FEF9A0D7EC5FDE4398ED29701A83C41158C109B7D0FB2A2E6DC649
7284F2E280667EBB44755367CA0BAD24BB51C25E348D886CECB3E0ED7EE72450
6C09BAF245696EB56C5DF4CEC29°¹...°Ä...t´°w05CFAA3AD1EBE¹...°Ä...t´°w5
F5D.Ä.w...w.0...G....°.....Ä.w...w.0...G....°.....%.....\¹...D
%...ä°µwÈ¹...\%...°...t¹...\%...0%µw\%...ô¹...°µwÈ¹...\%...°...t¹...%µwÈ
¹...°Ä...\%...w.°wÈ¹...°w°°w.°.....pŷŷŷ...ÄÄ.....€.....Ú...
```

## Impact

Auth data disclosure.

## CVE

CVE-2022-22908

## Credit

This issue was discovered and reported by Nicolas Fasolo (@Err0r0x41414141) team Owner of NF\_Security ([www.threatfeedservice.it](http://www.threatfeedservice.it)).

## Contact

---

You can contact the NF\_Security team at [info@threatfeedservice.it](mailto:info@threatfeedservice.it), please include a reference to CVE-2022-22908 in any communication regarding this topic.