Err0r0x41414141 Update Readme.md ... on Feb 26 History

..

Readme.md 9 months ago

Readme.md

Coordinated Disclosure Timeline

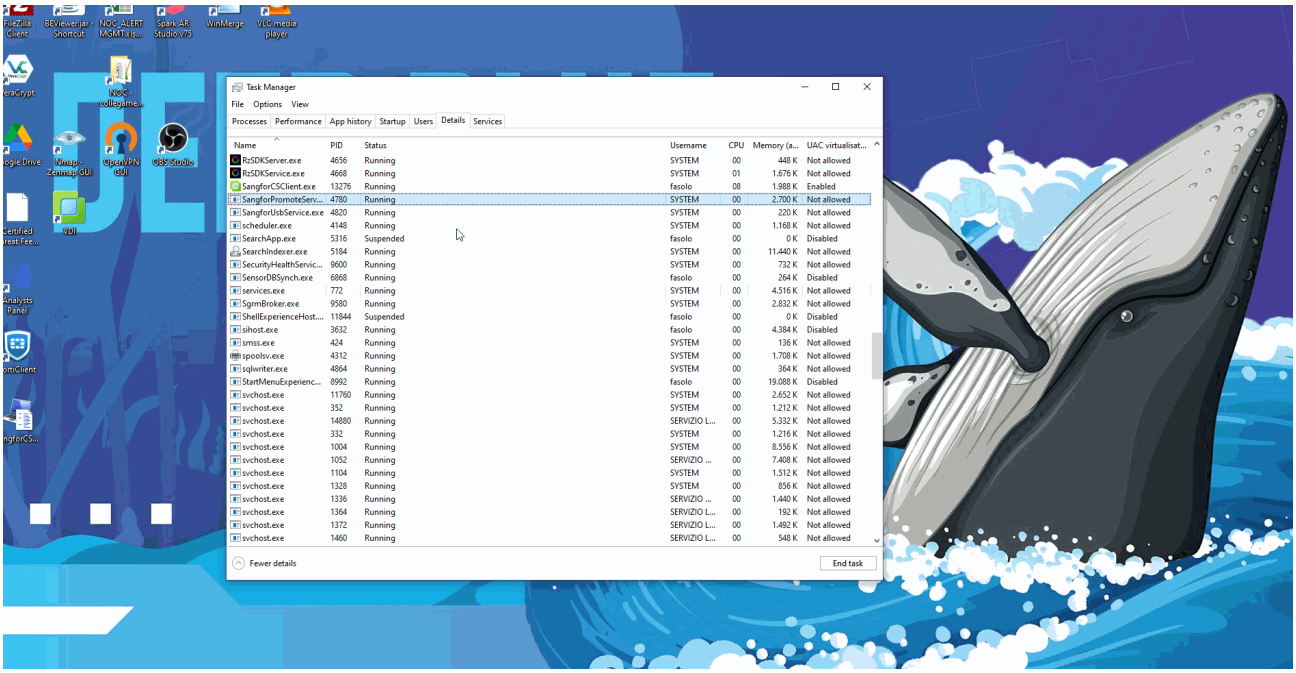
04/01/2022: Report submission to Vendor via Ticket
05/01/2022: Vendor acknowledged CVE and has been notified of my intention to publish the advisory
05/01/2022: CVE submission sent to MITRE.org
17/02/2022: CVE reservation "CVE-2022-22908"
26/02/2022: CVE advisory publishment via this repository

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

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).

Contact

You can contact the NF_Security team at info@threatfeedservice.it, please include a reference to CVE-2022-22908 in any communication regarding this topic.