

Shatter Attack

Privilege Escalation on Win32 Systems

Adrian Leuenberger

adrian.leuenberger-AT-csnc.ch

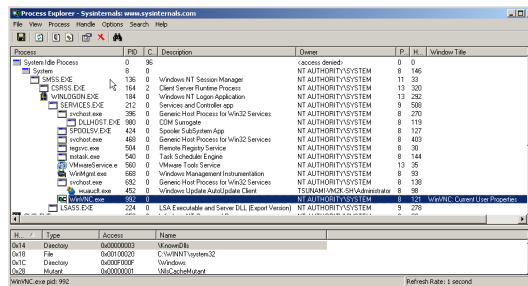
- Operating System: Windows 2000
- Service-Pack: SP2
- User: user2
- Group: Users

- How does an attacker get administrative rights on a host?

■ Processes

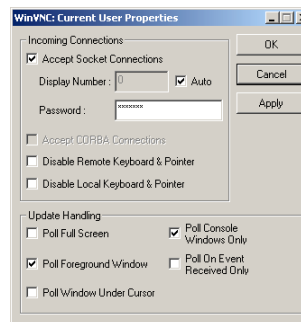
- Processes that only SYSTEM has access to
- Processes that are created by the user
- Processes that are created by SYSTEM, but live and can be manipulated by the logged on user

■ Demo: Process Explorer



■ Design Flaw in Messaging

- Any application can send messages to any other application on the same desktop. Regardless whether one application has permissions in the other application or not.
- Source/Destination of messages is not verified
- Any message can be sent
- Demo: WinVNC



1. WinVNC runs as „SYSTEM“

3. Window-Handle

2. Edit Box

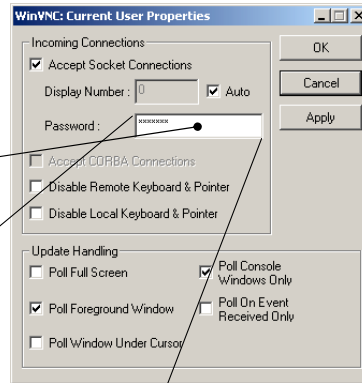
<identifier><.....nop slide.....><shell code>

5. WM_PASTE (exploit code)

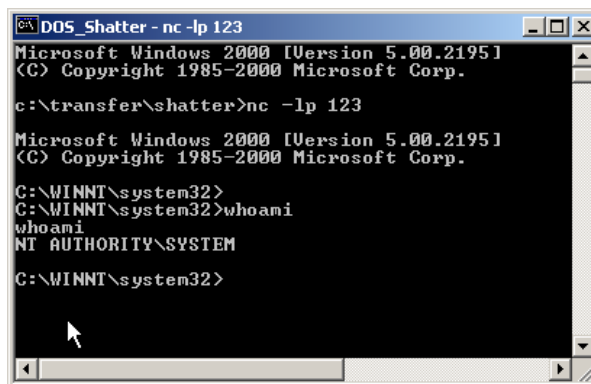
4. Modify size

6. Locate memory address

7. WM_TIMER (Callback address)
Callback address = Memory address + length(nopslide)/2



■ Demo: As a normal user



- How to prevent?
 - Administrators:
 - Do not give more rights than necessary to your users
 - Maintain a current patch level
 - Test the patches before deploying them!
 - Anti Virus ;-)
 - Developers:
 - Catch dangerous messages such as WM_TIMER
 - Design applications and API's carefully
 - Think about security from design to delivery

Questions ?

Compass Security Networking Computing AG
<http://www.csnc.ch>

Adrian Leuenberger
adrian.leuenberger-AT-csnc.ch

All slides are downloadable on our homepage next week.

- The Ten Immutable Laws of Security
<http://www.microsoft.com/technet/columns/security/essays/10imslaws.asp>
- Shatter Attacks – How to break Windows
<http://security.tombom.co.uk/shatter.html>
<http://security.tombom.co.uk/moreshatter.html>
- A New Avenue of Attack: Event-driven system vulnerabilities
http://www.isg.rhul.ac.uk/~simos/event_demo/