

## Local Privilege Escalation, DoS and other

*March 1, 2006. Ramon "ports" Kukla published a bug report on the NCP VPN/PKI Client. He reports 4 bugs that he had found in the software and he claims to be "sure that there are still some nice bugs".*

**Here is NCP's position statement on the bug report:**

### General

NCP emphasizes that the points listed in the article cited above are categorized as non-critical from the perspective of security, because in virtually all cases there must be direct physical access to the corresponding remote PC system. The points listed contain no possibilities whatsoever for external attackers to break the security of the central LAN. At no time is there a risk to the security of the connection between VPN Client and Gateway.

The denial of service attack is negligible in typical remote access scenarios (ISDN, UMTS, etc.). All other points would only have effects if an AUTHORIZED USER were to willfully sabotage his own system. Access to the central data network with this kind of sabotaged computer is prevented through the central NCP Secure Enterprise Management system.

Moreover the statement that the tester assumes that there certainly are "other nice errors" in the software, is speculative.

Below you will find an overview of the itemized points and the corresponding position statement from NCP:

### 1. Unnamed (-> Application-related firewall rules without hash)

This described phenomenon does not involve a defective function of the current NCP software, rather it involves a practical supplemental function that is being planned in NCP, and that will be introduced in a later NCP version.

### 2. Buffer Overflow with Privilege Escalation (some sort of), DoS

Example 1: Access to blocked Client Monitor menus (ncpmon.exe).

The phenomenon described by the tester is confirmed by NCP. Access to the NCP phonebook entries (= VPN connection information) of the NCP Secure Enterprise Client however does remain blocked, i.e. user name and password combination cannot be viewed or manipulated. Moreover it is impossible to change the firewall settings. A security risk for the central LAN, or for the client PC, due to possible manipulation possibilities of the Client Monitor, does not exist.

The described manipulation possibility is eliminated with the following Client versions:

- NCP Secure Enterprise Client 8.30 (release planned for March 2006)
- NCP Secure Entry Client 8.30 (release planned for March 2006)

Example 2: CPU load generation with ncprowsnt.exe via parameter transfer

There is no buffer overflow problem at this point, as noticed by the tester, neither is there any association with a parameter transfer. What is going on is that "ncprowsnt.exe" is called again by the AUTHORIZED USER, although it is already active as service. This causes two applications to listen to identical ports, which leads to the corresponding full load of the one. In practice this phenomenon can only be provoked by malicious behavior on the part of an AUTHORIZED USER, and thus it has no security-relevant effects whatsoever.

### **3. DoS, remote – high CPU load of "ncprwsnt.exe" at UDP packet bombardment with activated firewall**

The phenomenon described by the tester is confirmed by NCP. However it must be stated that the NCP Secure Client software is basically a remote access solution. Usually the probability of DoS attacks on the WAN segments (ISDN, UMTS, etc.) on remote clients is classified as low, in addition, low bandwidths are employed in this regard, through which these types of CPU loads of the client service do not occur. On the contrary in such cases the problem is more precisely due to exceeding the line capacity (e.g. ISDN, DSL), this is something that cannot be influenced on the computer itself by the software. A hazard to the central corporate LAN does not exist at any time.

Due to the higher number of incoming UDP packets the general load of the operating system increases, independently of the NCP Client Software, which causes generally slower operation.

### **4. Local Privilege Escalation – use of connect.bat and disconnect.bat**

Calling connect.bat and disconnect.bat with system rights is known to our customers, as well as to previously independent testers from other companies, and is used by a number of our customers in this form. If needed the administrator can prevent the user from utilizing connect.bat and disconnect.bat without authorization through the operating system's rights management.