

# [Full-disclosure] Microsoft ActiveSync information leak and spoofing

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0063.html>

---

*From:* 3APA3A (3APA3A\_at\_SECURITY.NNOV.RU)

*Date:* 08/02/05

Date: Tue, 2 Aug 2005 18:36:40 +0400

To: full-disclosure@lists.grok.org.uk, bugtraq@securityfocus.com, support@securiteam.com

Dear Bugtraq,

This vulnerability was reported by Natalia Melnikova  
(Hataha at yandex.ru)

Vulnerability: Microsoft ActiveSync information leak and spoofing

URL: <http://www.security.nnov.ru/Fnews64.html>

Vendor: Microsoft

Software: Active Sync 3.8

Author: Natalia Melnikova

Related Russian article:

"Microsoft ActiveSync (In)Security"

<http://www.securitylab.ru/56278.html>

-----

Microsoft ActiveSync clear text password

Microsoft ActiveSync is widely used to synchronise Windows based PDAs and smartphones with desktop computer. PDA can connect to PC via COM/USB/IR or LAN. Before synchronization user on PC must setup "partnership" to allow synchronization. If PDA is protected with password user on PC should provide password before he can access the device.

Synchronization over LAN has some design weakness.

1. All data, including initial "authentication", is transmitted in clear text. This is OK in case COM/USB and other physical protected communication, but LAN (Wi-Fi in most cases) is very sensitive for sniffing.
2. Even if PDA is password protected, ActiveSync doesn't ask password in case of network synchronization. I'm not sure, what is it – security bug or feature, because password is transmitted in clear text over USB.

## Full-Disclosure: [Full-disclosure] Microsoft ActiveSync information leak and spoofing

3. ActiveSync doesn't use any form of authentication for server (PC) or client (PDA), so fake server or fake client attack is possible.

Discover Activesync with LAN synchronization allowed

```
nmap -p 5679 192.168.0.*
```

Fake server

It is easy to build fake server attack without special software. All you need are ActiveSync, sniffer and any MitM condition.

1. Install ActiveSync on fake server. Enable network synchronization
2. Realize MitM condition.
3. Launch you favorite sniffer and set filter to save TCP packets on port 5679.
4. Wait for PDA connection.
5. Open sniffer and check second data packet from PDA. At offset 0x14 and 0x18 you can see partnerships ids. Activesync can support up to 2 PC and as you can see, PDA send both IDs in the "handshake"
6. Import template in registry. Change key HKEY\_CURRENT\_USER\Software\Microsoft\Windows CE Services\Partners\<Partnership> to sniffed partnership id.
7. Wait for another connection and check ActiveSinc, device should be connected as "guest". Even if you got "Synchronization Error", try to click "Explore" button on the toolbar.

Fake Client

Is very similar to the fake server, but you don't need MitM conditions to accomplish this attack. All you need it a name of PC and corresponding "partnership id".

1. Launch your favorite registry editor for Windows Mobile.
2. Navigate to HKLM\Software\Microsoft\Windows CE Services\Partners\P1
3. Create string value PName = <PC\_NAME>
4. Create DWORD value PId = <partnership id>
5. Launch active sync on PDA and try to connect. If everything is ok, synchronization will occur.

Mitigating factors

1. LAN synchronization disabled by default
2. To implement "fake client" you should know Partnership ID. It's hard to guess ( $2^{32}$ ), but because ActiveSync accept 2 partnership ID per connection, actually we need ( $2^{31}$ ) connections for bruteforce.

I think ActiveSync should use TLS for authentication of PC and PDA and data encryption. We don't need PKI in this case, because "direct trust" can be created and certificates transmitted from PDA to PC and vice versa when "Partnership" is established.

Thanks 2 3APA3A and everybody in SynCE project

---

Full-Disclosure – We believe in it.

Full-Disclosure: [Full-disclosure] Microsoft ActiveSync information leak and spoofing

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>