Submit #561145: PCMan FTP Server 2.0.7 Buffer Overflow

Title	**PCMan FTP Server 2.0.7 Buffer Overflow**
Description	This technique works well against Windows XP Professional Service Pack 2 and 3. For this exploit, I tried several strategies to increase the reliability of the Poc - Proof Of Concept. Sending an excessive amount of data through the "QUOTE" command, the application crashes, indicating the Buffer Overflow condition. Then, the offset amount was identified by using msf-pattern_create -l 3000 And then by using msf-pattern_offset -q to discover the offset amount. After discovering the offset amount, it was necessary to adjust the data in the stack. To advance in the exploit , mona was used, together with the command !mona jmp -r esp -n to discover a JMP ESP address, in this case it was 0x74e32fd9. Then I used the removal of the main badchars: 0x00\0x0a\0x0d I did not perform a search for badchars through bytearray, because I already knew the environment I was working in. Finally, I added 20 nops and generated the shellcode with msfvenom Successful exploitation of these issues could allow attackers to obtain a remote shell on the system.
Source	⚠️ https://fitoxs.com/exploit/exploit-81dc9bdb52d04dc20036dbd8313ed055.txt
User	Fernando Mengali (UID 83791)
Submission	04/17/2025 06:18 PM (16 days ago)
Moderation	05/01/2025 02:44 PM (14 days later)
Status	Accepted
VulDB Entry	306802 [PCMan FTP Server 2.0.7 QUOTE Command buffer overflow]
Points	20

⚠ Notice

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

? Documentation

- Submission Policy
- Data Processing
- CVE Handling