



VDB-307355 · CVE-2025-4251 · GCVE-100-307355

PCMAN FTP SERVER 2.0.7 RMDIR COMMAND BUFFER OVERFLOW

A vulnerability was found in PCMan FTP Server 2.0.7 and classified as critical. This issue affects some unknown processing of the component *RMDIR Command Handler*. The manipulation with an unknown input leads to a buffer overflow vulnerability. Using CWE to declare the problem leads to CWE-120. The product copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow. Impacted is confidentiality, integrity, and availability.

It is possible to read the advisory at fitoxs.com. The identification of this vulnerability is CVE-2025-4251. The exploitation is known to be easy. The attack may be initiated remotely. No form of authentication is needed for a successful exploitation. Technical details are unknown but a public exploit is available.

The exploit is available at fitoxs.com. It is declared as proof-of-concept.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Similar entries are available at VDB-307329, VDB-307330, VDB-307331 and VDB-307356.

Product

Type

- File Transfer Software

Vendor

- PCMan

Name

- FTP Server

Version

- 2.0.7

CPE 2.3

- 

CPE 2.2

- 

CVSSv4

VulDB Vector: 

VulDB Reliability: 

CNA CVSS-B Score: 

CNA CVSS-BT Score: 

CNA Vector: 

CVSSv3

VulDB Meta Base Score: 7.3

VulDB Meta Temp Score: 6.9

VulDB Base Score: 7.3

VulDB Temp Score: 6.6

VulDB Vector: 

VulDB Reliability: 

CNA Base Score: 7.3

CNA Vector: 

CVSSv2

VulDB		CNA		CVSSv2	
Base	Temp	Base	Temp	Base	Temp
7.3	6.6	7.3	6.6	7.3	6.6
7.3	6.6	7.3	6.6	7.3	6.6
7.3	6.6	7.3	6.6	7.3	6.6

VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

Exploiting

Class: Buffer overflow

CWE: CWE-120 / CWE-119

CAPEC: 

ATT&CK: 

Local: No

Remote: Yes

Availability: 

Access: Public

Status: Proof-of-Concept

Download: 

Price Prediction: 

Current Price Estimation: 



Threat Intelligence

Interest: 

Active Actors: 

Active APT Groups: 

Countermeasures

Recommended: no mitigation known

Status: 

0-Day Time: 

Timeline

05/04/2025		Advisory disclosed
05/04/2025	+0 days	VulDB entry created
05/05/2025	+0 days	VulDB entry last update

Sources

Advisory: fitoxs.com

Status: Not defined

CVE: CVE-2025-4251 ()

GCVE (CVE): GCVE-0-2025-4251

GCVE (VulDB): GCVE-100-307355

scip Labs: <https://www.scip.ch/en/?labs.20161013>

See also: 

Entry

Created: 05/04/2025 08:59 AM

Updated: 05/05/2025 01:37 AM

Changes: 05/04/2025 08:59 AM (55), 05/05/2025 01:37 AM (30)

Complete: 

Submitter: Fernando Mengali

Cache ID: 5:9F9:101

Submit

Accepted

- Submit #561597: PCMan FTP Server 2.0.7 Buffer Overflow (by Fernando Mengali)

Discussion

No comments yet. Languages: en.

Please log in to comment.