



VDB-307330 · CVE-2025-4239 · GCVE-100-307330

PCMAN FTP SERVER 2.0.7 TYPE COMMAND BUFFER OVERFLOW

A vulnerability was found in PCMan FTP Server 2.0.7. It has been declared as critical. This vulnerability affects some unknown functionality of the component *TYPE Command Handler*. The manipulation with an unknown input leads to a buffer overflow vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is available at fitoxs.com. This vulnerability was named CVE-2025-4239. The exploitation appears to be easy. The attack can be initiated remotely. No form of authentication is required for a successful exploitation. Technical details are unknown but a public exploit is available.

It is possible to download the exploit 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-306802, VDB-307327, VDB-307328 and VDB-307329.

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

CVSSv2	CVSSv3	CVSSv4	CVSSv2	CVSSv3	CVSSv4
7.3	7.3	7.3	7.3	7.3	7.3
6.6	6.6	6.6	6.6	6.6	6.6
7.3	7.3	7.3	7.3	7.3	7.3

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

05/02/2025		Advisory disclosed
05/02/2025	+0 days	VulDB entry created
05/03/2025	+1 days	VulDB entry last update

Sources

Advisory: fitoxs.com

Status: Not defined

CVE: CVE-2025-4239 ()

GCVE (CVE): GCVE-0-2025-4239

GCVE (VulDB): GCVE-100-307330

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

See also: 

Entry

Created: 05/02/2025 10:34 PM

Updated: 05/03/2025 08:35 PM

Changes: 05/02/2025 10:34 PM (55), 05/03/2025 08:35 PM (30)

Complete: 

Submitter: Fernando Mengali

Cache ID: 5:1CB:101

Submit

Accepted

- Submit #561562: PCMan FTP Server 2.0.7 Buffer Overflow (by Fernando Mengali)

Discussion

No comments yet. Languages: en.

Please log in to comment.