VDB-306804 · CVE-2025-4186 · GCVE-100-306804

WANGSHEN SECGATE 3600 2024 ?G=ROUTE_ISPINFO_EXPORT_SAVE FILE_NAME PATH TRAVERSAL

A vulnerability, which was classified as critical, was found in Wangshen SecGate 3600 2024. Affected is an unknown functionality of the file */?g=route_ispinfo_export_save*. The manipulation of the argument `file_name` with an unknown input leads to a path traversal vulnerability. CWE is classifying the issue as CWE-22. The product uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the product does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory. This is going to have an impact on confidentiality, integrity, and availability.

The advisory is shared for download at flowus.cn. This vulnerability is traded as CVE-2025-4186. The exploitability is told to be easy. It is possible to launch the attack remotely. Technical details and a public exploit are known. The MITRE ATT&CK project declares the attack technique as T1006.

The exploit is shared for download at flowus.cn. 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.

The entries VDB-186033, VDB-186034, VDB-213447 and VDB-221718 are related to this item.

Product

Vendor

- Wangshen

Name

- SecGate 3600

Version

- 2024

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: 6.3
VulDB Meta Temp Score: 6.0

VulDB Base Score: 6.3
VulDB Temp Score: 5.7
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 6.3
CNA Vector: 🔒

CVSSv2

VulDB Base Score: 🔒
VulDB Temp Score: 🔒
VulDB Reliability: 🔍

Exploiting

Class: Path traversal
CWE: CWE-22
CAPEC: 🔒

ATT&CK: 🔒

Local: No
Remote: Yes

Availability: 🔒
Access: Public
Status: Proof-of-Concept
Download: 🔒

EPSS Score: 🔒
EPSS Percentile: 🔒

Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍
Active Actors: 🔍
Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/01/2025		Advisory disclosed
05/01/2025	+0 days	VulDB entry created
05/02/2025	+1 days	VulDB entry last update

Sources

Advisory: flowus.cn
Status: Not defined

CVE: CVE-2025-4186 (🔒)
GCVE (CVE): GCVE-0-2025-4186
GCVE (VulDB): GCVE-100-306804

scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/01/2025 02:53 PM
Updated: 05/02/2025 10:52 AM
Changes: 05/01/2025 02:53 PM (55), 05/02/2025 10:52 AM (30)
Complete: 🔍
Submitter: 0menc
Cache ID: 5:22B:101

Submit

Accepted

- Submit #561814: Wangshen SecGate 3600 affected at 2024 Path Traversal (by 0menc)

Discussion

No comments yet. Languages: en.

Please log in to comment.