VDB-308275 · CVE-2025-4530 · GCVE-100-308275

FENG_HA_HA/MEGAGAO SSM-ERP/PRODUCTION_SSM 1.0 FILE FILECONTROLLER.JAVA HANDLEFILEDOWNLOAD PATH TRAVERSAL

A vulnerability was found in feng_ha_ha/megagao ssm-erp and production_ssm 1.0. It has been declared as problematic. Affected by this vulnerability is the function `handleFileDownload` of the file *FileController.java* of the component *File Handler*. The manipulation with an unknown input leads to a path traversal vulnerability. The CWE definition for the vulnerability is 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. As an impact it is known to affect confidentiality.

It is possible to read the advisory at github.com. This vulnerability is known as CVE-2025-4530. The exploitation appears to be easy. The attack can be launched remotely. Technical details and also a public exploit are known. The attack technique deployed by this issue is T1006 according to MITRE ATT&CK.

It is possible to download the exploit at github.com. It is declared as proof-of-concept. This product is distributed under two entirely different names.

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

Similar entry is available at VDB-211149.

Product

Type

- Enterprise Resource Planning Software

Vendor

- feng_ha_ha
- megagao

Name

- production_ssm
- ssm-erp

Version

- 1.0

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: 4.3
VulDB Meta Temp Score: 4.1

VulDB Base Score: 4.3
VulDB Temp Score: 3.9
VulDB Vector: 🔒
VulDB Reliability: 🔍

CNA Base Score: 4.3
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: 🔒
Price Prediction: 🔍
Current Price Estimation: 🔒

Threat Intelligence

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

Countermeasures

Recommended: no mitigation known
Status: 🔍

0-Day Time: 🔒

Timeline

05/10/2025		Advisory disclosed
05/10/2025	+0 days	VulDB entry created
05/11/2025	+1 days	VulDB entry last update

Sources

Advisory: github.com
Status: Not defined

CVE: CVE-2025-4530 (🔒)
GCVE (CVE): GCVE-0-2025-4530
GCVE (VulDB): GCVE-100-308275
scip Labs: https://www.scip.ch/en/?labs.20161013
See also: 🔒

Entry

Created: 05/10/2025 07:43 AM
Updated: 05/11/2025 07:40 AM
Changes: 05/10/2025 07:43 AM (58), 05/11/2025 07:40 AM (30)
Complete: 🔍
Submitter: fatd0g
Cache ID: 5:EB7:101

Submit

Accepted

- Submit #565380: production_ssm 1 Arbitrary File Reads (by fatd0g)

Discussion

No comments yet. Languages: en.

Please log in to comment.