

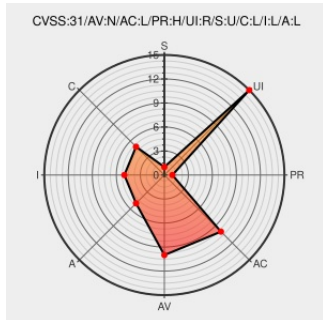


CVE-2022-28871

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:22:00 PM UTC

CVE-2022-28871

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Macos](#) from [Apple](#) contain the following vulnerability:

A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the fsicapd component used in certain F-Secure products while scanning larger packages/fuzzed files consume too much memory eventually can crash the scanning engine. The exploit can be triggered remotely by an attacker.

CVE-2022-28871 has been assigned by [f cve-notifications-us@f-secure.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [F-Secure](#) - All F-Secure Endpoint Protection products on Windows and Mac F-Secure Linux Security (32-bit) F-Secure Linux Security 64 F-Secure Atlant F-Secure Internet Gatekeeper F-Secure Cloud Protection for Salesforce version = All Version

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description

CVE-2022-28871 | F-Secure

CVE-2022-28871 - Denial-of-Service (DoS) Vulnerability | WithSecure™

Tags

www.f-secure.com

text/html

www.withsecure.com

text/html

Link

MISC www.f-secure.com/en/home/support/security-advisories/cve-2022-28871

MISC www.withsecure.com/en/support/security-advisories/cve-2022-28871

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Application	F-secure	Atlant	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

cpe:2.3:o:apple:macos:-:*:*:*:*:*:

cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:*:

cpe:2.3:a:f-secure:atlant:-:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-28871 : A Denial-of-Service #DoS vulnerability was discovered in F-Secure Atlant before 2022-04-12_01 wh... twitter.com/i/web/status/1...	2022-04-25 11:03:15
/r/netcve	CVE-2022-28871	2022-04-25 11:39:58

← Previous ID

Next ID →

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)