



CVE-2023-20197

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-20197
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-16 22:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	A vulnerability in the filesystem image parser for Hierarchical File System Plus (HFS+) of ClamAV could allow an unauthent

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Secure Endpoint	All	All	All	All
Application	Cisco	Secure Endpoint	All	All	All	All
Application	Cisco	Secure Endpoint	All	All	All	All
Application	Cisco	Secure Endpoint Private Cloud	All	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 38 Update: clamav-1.0.2-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
[SECURITY] [DLA 3544-1] clamav security update	MISC	lists.debian.org
[SECURITY] Fedora 37 Update: clamav-0.103.9-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
ClamAV HFS+ File Scanning Infinite Loop Denial of Service Vulnerability	MISC	sec.cloudapps.cisco.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199673](#) Ubuntu Security Notification for ClamAV Vulnerability (USN-6303-1)

[199674](#) Ubuntu Security Notification for ClamAV Vulnerability (USN-6303-2)

[284432](#) Fedora Security Update for clamav (FEDORA-2023-bf72d8833e)

[505992](#) Alpine Linux Security Update for clamav

[6000083](#) Debian Security Update for clamav (DLA 3544-1)

[691235](#) Free Berkeley Software Distribution (FreeBSD) Security Update for clamav (51a59f36-3c58-11ee-b32e-080027f5fec9)

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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