CVE-2023-20032

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2023-20032
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-01 08:15:00 UTC
Updated	2024-01-25 17:15:00 UTC
Description	On Feb 15, 2023, the following vulnerability in the ClamAV scanning library was disclosed: A vulnerability in the HFS+ partit

Risk And Classification

Problem Types: CWE-787

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
Application	Cisco	Web Security Appliance	All	All	All	All
Application	Clamav	Clamav	1.0.0	-	All	All
Application	Clamav	Clamav	1.0.0	rc	All	All
Application	Clamav	Clamav	1.0.0	rc2	All	All
Application	Clamav	Clamav	All	All	All	All
Application	Clamav	Clamav	All	All	All	All
Application	Stormshield	Stormshield Network Security	All	All	All	All

References

Reference	Source	Link
ClamAV HFS+ Partition Scanning Buffer Overflow Vulnerability Affecting Cisco Products: February 2023	MISC	sec.cloudapps.cisco.c
ClamAV: Multiple Vulnerabilities (GLSA 202310-01) — Gentoo security	MISC	security.gentoo.org
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

- 181595 Debian Security Update for clamav (DLA 3328-1)
- 184092 Debian Security Update for clamav (CVE-2023-20032)
- 199187 Ubuntu Security Notification for ClamAV Vulnerabilities (USN-5887-1)
- 283722 Fedora Security Update for clamav (FEDORA-2023-d686b8d48f)
- 283724 Fedora Security Update for clamav (FEDORA-2023-3ba365d538)
- 317318 Cisco Secure Web Appliance Buffer Overflow Vulnerability (CSCwd74132)
- 354748 Amazon Linux Security Advisory for clamav : ALAS-2023-1694
- 354777 Amazon Linux Security Advisory for clamav : ALAS2-2023-1964
- 355247 Amazon Linux Security Advisory for clamav : ALAS2023-2023-112
- 378338 Zimbra Collaboration ClamAV Package Vulnerability
- 378545 Cisco Advanced Malware Protection (AMP) Buffer Overflow Vulnerability (cisco-sa-clamav-q8DThCy)
- 378767 ClamAV Multiple Vulnerabilities (CVE-2023-20032 and CVE-2023-20052)
- 502833 Alpine Linux Security Update for clamav
- 503152 Alpine Linux Security Update for clamav
- 505991 Alpine Linux Security Update for clamav
- 691062 Free Berkeley Software Distribution (FreeBSD) Security Update for clamav (fd792048-ad91-11ed-a879-080027f5fec9)
- 710761 Gentoo Linux ClamAV Multiple Vulnerabilities (GLSA 202310-01)
- 753723 SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2023:0453-1)
- 753774 SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2023:0471-1)
- 753775 SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2023:0471-1)
- 753776 SUSE Enterprise Linux Security Update for clamav (SUSE-SU-2023:0470-1)
- 905645 Common Base Linux Mariner (CBL-Mariner) Security Update for clamav (13724)
- 905693 Common Base Linux Mariner (CBL-Mariner) Security Update for clamav (13724-1)
- 906676 Common Base Linux Mariner (CBL-Mariner) Security Update for clamav (13724-3)