



CVE-2019-1010060

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

Summary

CVE	CVE-2019-1010060
State	PUBLIC
Assigner	cve-assign@distributedweaknessfiling.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-16 13:15:00 UTC
Updated	2019-07-22 18:00:00 UTC
Description	NASA CFITSIO prior to 3.43 is affected by: Buffer Overflow. The impact is: arbitrary code execution. The component is: ove

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nasa	Cfitsio	All	All	All	All
Application	Nasa	Cfitsio	All	All	All	All

References

Reference	Source	Link
heasarc.gsfc.nasa.gov/FTP/software/fitsio/c/cfitsio3420.tar.gz	MISC	heasarc.gsfc.nasa
#892458 - cfitsio: vulnerabilities - Debian Bug report logs	MISC	bugs.debian.org
heasarc.gsfc.nasa.gov/FTP/software/fitsio/c/docs/changes2.txt	MISC	heasarc.gsfc.nasa
heasarc.gsfc.nasa.gov/FTP/software/fitsio/c/cfitsio3430.tar.gz	MISC	heasarc.gsfc.nasa
Update cfitsio to v3.43: includes critical bug fix by drdavella · Pull Request #7274 · astropy/astropy · GitHub	MISC	github.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.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

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