



CVE-2018-3848

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-3848
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-04-16 16:29:00 UTC
Updated	2023-11-07 02:58:00 UTC
Description	In the ffghbn function in NASA CFITSIO 3.42, specially crafted images parsed via the library can cause a stack-based buffer overflow.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Application	Nasa	Cfitsio	All	All	All	All
Application	Nasa	Cfitsio	All	All	All	All

References

Reference	Source	Link	Type
[SECURITY] Fedora 28 Update: cfitsio-3.430-2.fc28 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	T
[SECURITY] Fedora 28 Update: cfitsio-3.430-2.fc28 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	M
TALOS-2018-0531 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	www.talosintelligence.com	E
cfitsio: Multiple vulnerabilities (GLSA 202101-24) — Gentoo security	GENTOO	security.gentoo.org	T
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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](#)