



CVE-2019-5086

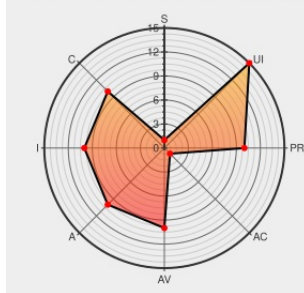
Published on: 11/21/2019 12:00:00 AM UTC

Last Modified on: 06/21/2022 07:22:00 PM UTC

CVE-2019-5086

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

CVSS:30/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An exploitable integer overflow vulnerability exists in the `flattenIncrementally` function in the `xcf2png` and `xcf2pnm` binaries of `xcftools`, version 1.0.7. An integer overflow can occur while walking through tiles that could be exploited to corrupt memory and execute arbitrary code. In order to trigger this vulnerability, a victim would need to open a specially crafted XCF file.

CVE-2019-5086 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 2553-1] xcftools security update	Mailing List Third Party Advisory	MLIST [debian-lts-announce] 20210210 [SECURITY] [DLA 2553-1] xcftools security update

	lists.debian.org text/html	
TALOS-2019-0878 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory www.talosintelligence.com text/html	 MISC www.talosintelligence.com/vulnerability_reports/TALOS-2019-0878
TALOS-2019-0878 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	 MISC talosintelligence.com/vulnerability_reports/TALOS-2019-0878
[SECURITY] [DLA 2553-2] xcftools regression update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20210308 [SECURITY] [DLA 2553-2] xcftools regression update

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.

Related QID Numbers

199266 Ubuntu Security Notification for Xcftools Vulnerabilities (USN-5988-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Xcftools Project	Xcftools	1.0.7	All	All	All
Application	Xcftools Project	Xcftools	1.0.7	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:xcftools_project:xcftools:1.0.7:*:*:*:*:*:						
cpe:2.3:a:xcftools_project:xcftools:1.0.7:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
← Previous IDNext ID →		

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](#)