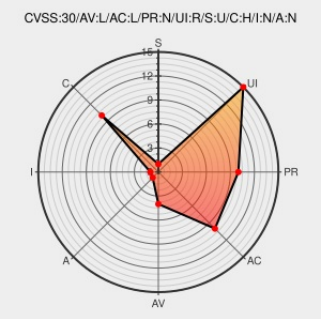
CVE-2018-11723

Published on: 06/19/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:18 PM UTC

CVE-2018-11723

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libpff from Libpff Project contain the following vulnerability:

** DISPUTED ** The libpff_name_to_id_map_entry_read function in libpff_name_to_id_map.c in libyal libpff through 2018-04-28 allows remote attackers to cause an information disclosure (heap-based buffer over-read) via a crafted pff file. NOTE: the vendor has disputed this as described in libyal/libpff issue 66 on GitHub.

CVE-2018-11723 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 1.9 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Full Disclosure: libpff 20180428 vulnerability	Mailing List, Third Party Advisory, seclists.org	FULLDISC 20180608 libpff 20180428 vulnerability

	text/html	
libpff 2018-04-28 Information Disclosure ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/148113/libpff-2018-04-28-Information-Disclosure.html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libpff Project	Libpff	All	All	All	All

cpe:2.3:a:libpff_project:libpff:*:*:*:*:*:*:*:*:

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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