



CVE-2007-2956

Published on: 08/13/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:42 PM UTC

CVE-2007-2956

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Pfstools** from **Pfstools** contain the following vulnerability:

Stack-based buffer overflow in the readRadianceHeader function in (1) src/fileformat/rgbeio.cpp in pfstools 1.6.2 and (2) src/Fileformat/rgbeio.cpp in Qtpfsgui 1.8.11 allows remote attackers to execute arbitrary code via a crafted Radiance RGBE (.hdr) file.

CVE-2007-2956 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

CVS Info for project pfstools

pfstools.cvs.sourceforge.net
text/html

CONFIRM
pfstools.cvs.sourceforge.net/pfstools/pfstools/src/fileformat/rgbeio.cpp?r1=1.8&r2=1.9

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

XF pfstools-readradianceheader-bo(35949)

No Description Provided

Patch
umdl.sourceforge.net

CONFIRM umdl.sourceforge.net/sourceforge/qtspfsgui/qtspfsgui-1.8.12.tar.gz

Inactive Link Not Archived

pfstools "readRadianceHeader()" Buffer Overflow Vulnerability - Advisories - Secunia

Vendor Advisory
web.archive.org
text/html

SECUNIA 26388

CVS Info for project pfstools

pfstools.cvs.sourceforge.net

CONFIRM

	text/html	pfstools.cvs.sourceforge.net/pfstools/pfstools/src/fileformat/rgbeio.cpp?revision=1.9&view=markup
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2007-2855
Qt pfsgui "readRadianceHeader()" Buffer Overflow Vulnerability - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 26387
About Secunia Research Flexera	Vendor Advisory web.archive.org text/html	 MISC secunia.com/secunia_research/2007-68/advisory/
Security Announcement	web.archive.org text/html Inactive Link Not Archived	 SUSE SUSE-SR:2007:018
pfstools "readRadianceHeader()" Buffer Overflow Vulnerability - Secunia Research - Secunia	Vendor Advisory web.archive.org text/html	 MISC secunia.com/secunia_research/2007-67/advisory/
SUSE Updates for Multiple Packages - Advisories - Secunia	web.archive.org text/html	 SECUNIA 26674
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF qt pfsgui-readradianceheader-bo(35948)
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2007-2856

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	Pfstools	Pfstools	1.6.2	All	All	All
Application	Pfstools	Pfstools	1.6.2	All	All	All
Application	Qt pfsgui	Qt pfsgui	1.8.11	All	All	All
Application	Qt pfsgui	Qt pfsgui	1.8.11	All	All	All
cpe:2.3:a:pfstools:pfstools:1.6.2:*:*:*:*:*:						
cpe:2.3:a:pfstools:pfstools:1.6.2:*:*:*:*:*:						
cpe:2.3:a:qt pfsgui:qt pfsgui:1.8.11:*:*:*:*:*:						
cpe:2.3:a:qt pfsgui:qt pfsgui:1.8.11:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

© [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 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](#)