CVE-2021-4214

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-4214
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-24 16:15:00 UTC
Updated	2022-11-08 02:32:00 UTC
Description	A heap overflow flaw was found in libpngs' pngimage.c program. This flaw allows an attacker with local network access to p

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Libpng	Libpng	1.6.0	-	All	All
Application	Netapp	Ontap Select Deploy Administration Utility	-	All	All	All

References

Reference	Source	Link	Ta
A potential heap overflow issue · Issue #302 · glennrp/libpng · GitHub	MISC	github.com	
CVE-2021-4214	MISC	security-tracker.debian.org	
CVE-2021-4214 Libpng Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
2043393 – (CVE-2021-4214) CVE-2021-4214 libpng: hardcoded value leads to heap-overflow	MISC	bugzilla.redhat.com	
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

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 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**