



# CVE-2018-14550

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2018-14550
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-07-10 12:15:00 UTC
<b>Updated</b>	2023-03-01 01:57:00 UTC
<b>Description</b>	An issue has been found in third-party PNM decoding associated with libpng 1.6.35. It is a stack-based buffer overflow in th

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Libpng</a>	<a href="#">Libpng</a>	1.6.35	All	All	All
Application	<a href="#">Libpng</a>	<a href="#">Libpng</a>	1.6.35	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Oncommand Api Services</a>	-	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Hyperion Infrastructure Technology</a>	11.1.2.6.0	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Mysql Workbench</a>	All	All	All	All

## References

Reference	Source	Link	Tags
stack-buffer-overflow in pnm2png in function get_token · Issue #246 · glennrp/libpng · GitHub	MISC	<a href="#">github.com</a>	Exploit, Pa
libpng: Multiple vulnerabilities (GLSA 201908-02) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	
security/libpng at master · fouzhe/security · GitHub	MISC	<a href="#">github.com</a>	Exploit, Pa
Oracle Critical Patch Update Advisory - October 2021	MISC	<a href="#">www.oracle.com</a>	
CVE-2018-14550 libpng Vulnerability in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>	
Oracle Critical Patch Update Advisory - April 2021	MISC	<a href="#">www.oracle.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical,

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[500309](#) Alpine Linux Security Update for libpng

[504076](#) Alpine Linux Security Update for libpng

[710157](#) Gentoo Linux libpng Multiple vulnerabilities (GLSA 201908-02)

[980292](#) Dotnet (nuget) Security Update for libpng (GHSA-qwwr-qc2p-6283)

© [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](#)