



# CVE-2018-25012

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

## Summary

<b>CVE</b>	CVE-2018-25012
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-21 17:15:00 UTC
<b>Updated</b>	2023-02-28 15:46:00 UTC
<b>Description</b>	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in GetLE24().

## Risk And Classification

**Problem Types:** CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Ontap Select Deploy Administration Utility</a>	-	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Application	<a href="#">Webmproject</a>	<a href="#">Libwebp</a>	All	All	All	All

## References

Reference	Source	Link
9123 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	<a href="#">bugs.chromium.org</a>
[SECURITY] [DLA 2672-1] libwebp security update	MLIST	<a href="#">lists.debian.org</a>
May 2021 Libwebp Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="#">security.netapp.com</a>
[SECURITY] [DLA 2677-1] libwebp security update	MLIST	<a href="#">lists.debian.org</a>
95fd65070662e01cc9170c4444f5c0859a710097 - webm/libwebp - Git at Google	MISC	<a href="#">chromium.google.com</a>
1956922 - (CVE-2018-25012) CVE-2018-25012 libwebp: out-of-bounds read in WebPMuxCreateInternal()	MISC	<a href="#">bugzilla.redhat.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159474](#) Oracle Enterprise Linux Security Update for libwebp (ELSA-2021-4231)

[178659](#) Debian Security Update for libwebp (DLA 2672-1)

[178660](#) Debian Security Update for libwebp (DLA 2677-1)

[198390](#) Ubuntu Security Notification for libwebp vulnerabilities (USN-4971-1)

[239782](#) Red Hat Update for libwebp (RHSA-2021:4231)

[670580](#) EulerOS Security Update for libwebp (EulerOS-SA-2021-2338)

[670645](#) EulerOS Security Update for libwebp (EulerOS-SA-2021-2403)

[671012](#) EulerOS Security Update for libwebp (EulerOS-SA-2021-2594)

[750093](#) SUSE Enterprise Linux Security Update for libwebp (SUSE-SU-2021:1830-1)

[750108](#) SUSE Enterprise Linux Security Update for libwebp (SUSE-SU-2021:1860-1)

[750807](#) OpenSUSE Security Update for libwebp (openSUSE-SU-2021:1860-1)

[900015](#) CBL-Mariner Linux Security Update for libwebp 1.0.0

[902925](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libwebp (4209)

[940178](#) AlmaLinux Security Update for libwebp (ALSA-2021:4231)

[960323](#) Rocky Linux Security Update for libwebp (RLSA-2021:4231)

© [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](#)