

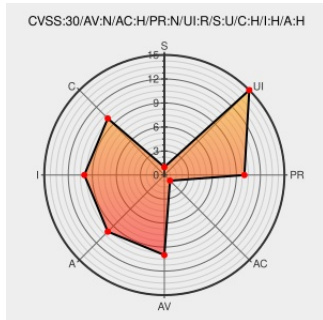


# CVE-2017-14449

Published on: 04/24/2018 12:00:00 AM UTC

Last Modified on: 04/19/2022 07:15:00 PM UTC

## CVE-2017-14449

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

A double-Free vulnerability exists in the XCF image rendering functionality of SDL2\_image-2.0.2. A specially crafted XCF image can cause a Double-Free situation to occur. An attacker can display a specially crafted image to trigger this vulnerability.

CVE-2017-14449 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [Cisco](#) **Sam Lantinga and Mattias Engdegård - Simple DirectMedia Layer** version **SDL2\_image 2.0.2**

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                | Tags                                                                                                      | Link                            |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|---------------------------------|
| Debian -- Security Information -- DSA-4177-1 libSDL2-image | <a href="#">Third Party Advisory</a><br><a href="#">www.debian.org</a><br><a href="#">Deprecated Link</a> | <a href="#">DEBIAN DSA-4177</a> |

Exploited? [Yes](#)  
text/html

TALOS-2017-0498 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

Technical Description  
Third Party Advisory  
[www.talosintelligence.com](http://www.talosintelligence.com)  
text/html

 MISC  
[www.talosintelligence.com/vulnerability\\_reports/TALOS-2017-0498](http://www.talosintelligence.com/vulnerability_reports/TALOS-2017-0498)

SDL2\_Image: Multiple vulnerabilities (GLSA 201903-17) — Gentoo security

Third Party Advisory  
[security.gentoo.org](http://security.gentoo.org)  
text/html

 GENTOO GLSA-201903-17

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](mailto:comment@cve.report).

## Related QID Numbers

[501247](#) Alpine Linux Security Update for sdl2\_image

[710189](#) Gentoo Linux SDL2\_Image Multiple vulnerabilities (GLSA 201903-17)

## Known Affected Configurations (CPE V2.3)

| Type                                         | Vendor                 | Product                      | Version | Update | Edition | Language |
|----------------------------------------------|------------------------|------------------------------|---------|--------|---------|----------|
| Operating System                             | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System                             | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Operating System                             | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 8.0     | All    | All     | All      |
| Operating System                             | <a href="#">Debian</a> | <a href="#">Debian Linux</a> | 9.0     | All    | All     | All      |
| Application                                  | <a href="#">Libsdl</a> | <a href="#">Sdl Image</a>    | 2.0.2   | All    | All     | All      |
| Application                                  | <a href="#">Libsdl</a> | <a href="#">Sdl Image</a>    | 2.0.2   | All    | All     | All      |
| cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*: |                        |                              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*: |                        |                              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*: |                        |                              |         |        |         |          |
| cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*: |                        |                              |         |        |         |          |
| cpe:2.3:a:libsdl:sdl_image:2.0.2:*:*:*:*:*:  |                        |                              |         |        |         |          |
| cpe:2.3:a:libsdl:sdl_image:2.0.2:*:*:*:*:*:  |                        |                              |         |        |         |          |

No vendor comments have been submitted for this CVE

[← 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 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](#)