



# CVE-2017-14440

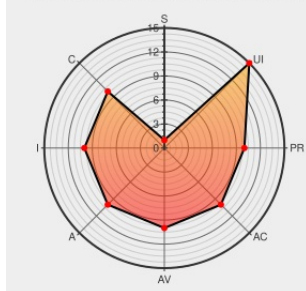
Published on: 04/24/2018 12:00:00 AM UTC

Last Modified on: 12/09/2022 02:07:00 AM UTC

## CVE-2017-14440

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

CVSS:30/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



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

An exploitable code execution vulnerability exists in the ILBM image rendering functionality of SDL2\_image-2.0.2. A specially crafted ILBM image can cause a stack overflow resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.

CVE-2017-14440 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                                                            |
|-----------------------------------------------|--------------------------------------|-----------------------------------------------------------------|
| [SECURITY] [DLA 1341-1] sdl-image1.2 security | <a href="#">Third Party Advisory</a> | <a href="#">MLIST [debian-lts-announce] 20180406 [SECURITY]</a> |

|                                                                                       |                                                                                                           |                                                                                                                                                           |
|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| update                                                                                | <div>lists.debian.org</div> <div>text/html</div>                                                          | [DLA 1341-1] sdl-image1.2 security update                                                                                                                 |
| Debian -- Security Information -- DSA-4177-1 libsd2-image                             | <div>Third Party Advisory</div> <div>www.debian.org</div> <div>Deprecated Link</div> <div>text/html</div> |  DEBIAN DSA-4177                                                         |
| TALOS-2017-0489    Cisco Talos Intelligence Group - Comprehensive Threat Intelligence | <div>Third Party Advisory</div> <div>www.talosintelligence.com</div> <div>text/html</div>                 |  MISC<br>www.talosintelligence.com/vulnerability_reports/TALOS-2017-0489 |
| SDL2_Image: Multiple vulnerabilities (GLSA 201903-17) — Gentoo security               | <div>Third Party Advisory</div> <div>security.gentoo.org</div> <div>text/html</div>                       |  GENTOO GLSA-201903-17                                                   |
| Debian -- Security Information -- DSA-4184-1 sdl-image1.2                             | <div>Third Party Advisory</div> <div>www.debian.org</div> <div>Deprecated Link</div> <div>text/html</div> |  DEBIAN DSA-4184                                                         |

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                              | Debian | Debian Linux | 7.0     | All    | All     | All      |
| Operating System                              | Debian | Debian Linux | 8.0     | All    | All     | All      |
| Operating System                              | Debian | Debian Linux | 9.0     | All    | All     | All      |
| Operating System                              | Debian | Debian Linux | 7.0     | All    | All     | All      |
| Operating System                              | Debian | Debian Linux | 8.0     | All    | All     | All      |
| Operating System                              | Debian | Debian Linux | 9.0     | All    | All     | All      |
| Application                                   | Libsdl | Sdl Image    | 2.0.2   | All    | All     | All      |
| Application                                   | Libsdl | Sdl Image    | 2.0.2   | All    | All     | All      |
| cpe:2.3:o:debian:debian_linux:7.0:****:*:*:*: |        |              |         |        |         |          |
| 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:7.0:*****: |
| 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 →