

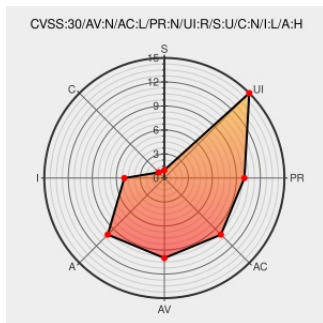


CVE-2017-14450

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

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

CVE-2017-14450

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

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

A buffer overflow vulnerability exists in the GIF image parsing functionality of SDL2_image-2.0.2. A specially crafted GIF image can lead to a buffer overflow on a global section. An attacker can display an image to trigger this vulnerability.

CVE-2017-14450 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: **7.1 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	HIGH

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 1341-1] sdl-image1.2 security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20180406 [SECURITY] [DLA 1341-1] sdl-image1.2 security update

Debian -- Security Information -- DSA-4177-1 libSDL2-image	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4177
TALOS-2017-0499 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Technical Description Third Party Advisory www.talosintelligence.com text/html	 MISC www.talosintelligence.com/vulnerability_reports/TALOS-2017-0499
SDL2_Image: Multiple vulnerabilities (GLSA 201903-17) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201903-17
Debian -- Security Information -- DSA-4184-1 sdl-image1.2	Third Party Advisory www.debian.org Deprecated Link text/html	 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.

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 →