



CVE-2018-3838

Published on: 04/10/2018 12:00:00 AM UTC

Last Modified on: 02/04/2023 01:08:00 AM UTC

CVE-2018-3838

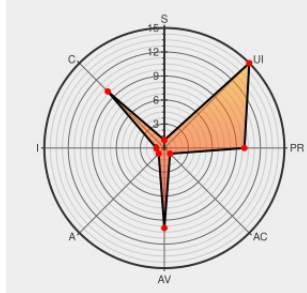
Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: PDF

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



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

An exploitable information vulnerability exists in the XCF image rendering functionality of Simple DirectMedia Layer SDL2_image-2.0.2. A specially crafted XCF image can cause an out-of-bounds read on the heap, resulting in information disclosure. An attacker can display a specially crafted image to trigger this vulnerability.

CVE-2018-3838 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cisco Systems, Inc.](#) - **Simple DirectMedia** version **Simple DirectMedia Layer SDL2_image 2.0.2**

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-4177-1 libSDL2-	Third Party Advisory	DEBIAN DSA-4177

image	www.debian.org Deprecated Link text/html	
TALOS-2018-0520 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Technical Description Third Party Advisory www.talosintelligence.com text/html	 MISC www.talosintelligence.com/vulnerability_reports/TALOS-2018-0520
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

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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	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: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](#)