

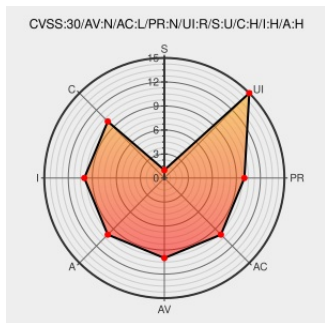


CVE-2018-3977

Published on: 11/01/2018 12:00:00 AM UTC

Last Modified on: 04/19/2022 07:10:47 PM UTC

CVE-2018-3977

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

Certain versions of [Sdl Image](#) from [Libsdl](#) contain the following vulnerability:

An exploitable code execution vulnerability exists in the XCF image rendering functionality of SDL2_image-2.0.3. A specially crafted XCF image can cause a heap overflow, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.

CVE-2018-3977 has been assigned by [cisco](#) talos-cna@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [cisco](#) **Simple DirectMedia Layer - Simple DirectMedia Layer** version **Simple DirectMedia Layer** **SDL2_image 2.0.3**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
-------------	------	------

USN-4238-1: SDL_image vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	 UBUNTU USN-4238-1
[SECURITY] [DLA 1861-1] libSDL2-image security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20190722 [SECURITY] [DLA 1861-1] libSDL2-image security update
TALOS-2018-0645 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit Third Party Advisory talosintelligence.com text/html	 MISC talosintelligence.com/vulnerability_reports/TALOS-2018-0645
SDL2_Image: Multiple vulnerabilities (GLSA 201903-17) — Gentoo security	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201903-17
[SECURITY] [DLA 1865-1] sdl-image1.2 security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20190727 [SECURITY] [DLA 1865-1] sdl-image1.2 security update

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
Application	Libsdl	Sdl Image	2.0.3	All	All	All
Application	Libsdl	Sdl Image	2.0.3	All	All	All
cpe:2.3:a:libsdl:sdl_image:2.0.3:*****:						
cpe:2.3:a:libsdl:sdl_image:2.0.3:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →