



CVE-2018-3839

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

Last Modified on: 10/25/2022 04:53:00 PM UTC

CVE-2018-3839

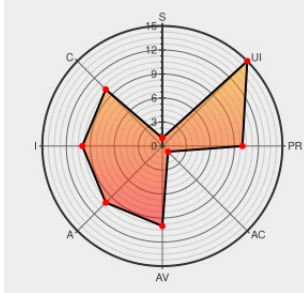
Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)

CVSS:30/AV:N/AC:H/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 XCF image rendering functionality of Simple DirectMedia Layer SDL2_image-2.0.2. A specially crafted XCF image can cause an out-of-bounds write on the heap, resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.

CVE-2018-3839 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

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

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

image	www.debian.org Deprecated Link text/html	
CVE-2018-3839 SDL2 vulnerability in StarWind VSAN for vSphere (VSA)	www.starwindsoftware.com text/html	 MISC www.starwindsoftware.com/security/sw-20191008-0002/
TALOS-2018-0521 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-2018-0521
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
Application	Starwindsoftware	Starwind Virtual San	v8	build12533	All	All
Application	Starwindsoftware	Starwind Virtual San	v8	build12658	All	All
Application	Starwindsoftware	Starwind Virtual San	v8	build12859	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:*:*:*:*:*:
cpe:2.3:a:starwindsoftware:starwind_virtual_san:v8:build12533:*:*:*:vsphere:*:*:
cpe:2.3:a:starwindsoftware:starwind_virtual_san:v8:build12658:*:*:*:vsphere:*:*:
cpe:2.3:a:starwindsoftware:starwind_virtual_san:v8:build12859:*:*:*:vsphere:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)