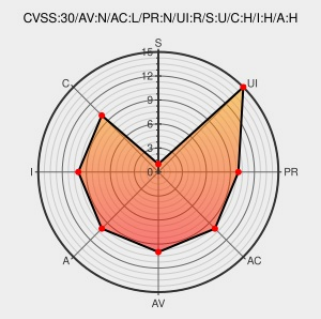
CVE-2017-14441

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

Last Modified on: 12/09/2022 02:10:00 AM UTC

CVE-2017-14441

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

An exploitable code execution vulnerability exists in the ICO image rendering functionality of SDL2_image-2.0.2. A specially crafted ICO image can cause an integer overflow, cascading to a heap overflow resulting in code execution. An attacker can display a specially crafted image to trigger this vulnerability.

CVE-2017-14441 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **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
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
[SECURITY] [DLA 1341-1] sdl-image1.2 security	Third Party Advisory	MLIST [debian-lts-announce] 20180406 [SECURITY]

update	lists.debian.org text/html	[DLA 1341-1] sdl-image1.2 security update
Debian -- Security Information -- DSA-4177-1 libsdl2-image	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-4177
TALOS-2017-0490 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory www.talosintelligence.com text/html	MISC www.talosintelligence.com/vulnerability_reports/TALOS-2017-0490
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 Depreciated Link text/html	DEBIAN DSA-4184

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→