

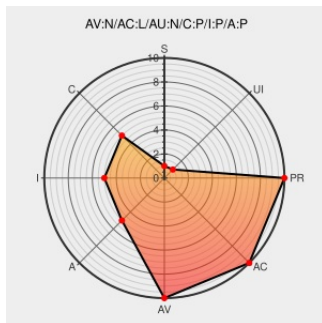


CVE-2002-2060

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:05 PM UTC

CVE-2002-2060

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

Certain versions of [Links](#) from [Twibright Labs](#) contain the following vulnerability:

Buffer overflow in Links 2.0 pre4 allows remote attackers to crash client browsers and possibly execute arbitrary code via gamma tables in large 16-bit PNG images.

CVE-2002-2060 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Twibright Labs Links Large PNG Image
Buffer Overflow Vulnerability

[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 4921](#)

ISS X-Force Database: links-png-image-bo (9287): Links Web browser large PNG image buffer overflow

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[🌐](#) [XF links-png-image-bo\(9287\)](#)

404 Not Found

[atrey.karlin.mff.cuni.cz](#)
[text/plain](#)
[Inactive Link](#) [Not Archived](#)

[🌐](#) [CONFIRM](#)
[atrey.karlin.mff.cuni.cz/~clock/twibright/links/download/ChangeLog](#)

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Twibright Labs	Links	2.0_pre4	All	All	All
Application	Twibright Labs	Links	2.0_pre4	All	All	All
cpe:2.3:a:twibright_labs:links:2.0_pre4:****:*:*:						
cpe:2.3:a:twibright_labs:links:2.0_pre4:****:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)