



# CVE-2016-9601

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2016-9601
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-24 01:29:00 UTC
<b>Updated</b>	2023-11-07 02:37:00 UTC
<b>Description</b>	ghostscript before version 9.21 is vulnerable to a heap based buffer overflow that was found in the ghostscript jbig2_decode

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Artifex	Gpl Ghostscript	All	All	All	All
Application	Artifex	Gpl Ghostscript	All	All	All	All
Application	Artifex	Jbig2dec	All	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	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

## References

Reference	Source
Ghostscript CVE-2016-9601 Local Integer Overflow Vulnerability	BID
git.ghostscript.com Git - jbig2dec.git/commit	
git.ghostscript.com Git - jbig2dec.git/commit	CONF
Bug 697457 – jbig2dec-0.13 Heap Buffer Overflow Vulnerability (READ\WRITE) due to Integer Overflow in function jbig2_image_new	CONF
Debian -- Security Information -- DSA-3817-1 jbig2dec	DEBI
1410021 – (CVE-2016-9601) CVE-2016-9601 ghostscript: Heap-buffer overflow due to Integer overflow in jbig2_image_new function	MISC
jbig2dec: Multiple vulnerabilities (GLSA 201706-24) — Gentoo security	GENT

CVE Program record

CVE

NVD vulnerability detail

NVD

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[670614](#) EulerOS Security Update for ghostscript (EulerOS-SA-2021-2372)

[710476](#) Gentoo Linux jbig2dec Multiple Vulnerabilities (GLSA 201706-24)

© [CVE.report](#) 2026 |

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](#)