



# CVE-2018-19134

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

## Summary

<b>CVE</b>	CVE-2018-19134
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-12-20 23:29:00 UTC
<b>Updated</b>	2023-11-07 02:55:00 UTC
<b>Description</b>	In Artifex Ghostscript through 9.25, the setpattern operator did not properly validate certain types. A specially crafted PostS

## Risk And Classification

**Problem Types:** CWE-704

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Artifex</a>	<a href="#">Ghostscript</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link	Tags
[SECURITY] [DLA 1620-1] ghostscript security update	MLIST	<a href="#">lists.debian.org</a>	Third Party Advisory

Recent Changes in Ghostscript	CONFIRM	<a href="http://www.ghostscript.com">www.ghostscript.com</a>	Release Notes
Ghostscript Vulnerabilities in Postscript & PDF Processings   Semmler Blog	MISC	<a href="http://semmler.com">semmler.com</a>	Exploit, Third Party Advis
Red Hat Customer Portal	REDHAT	<a href="http://access.redhat.com">access.redhat.com</a>	Third Party Advisory
Access Denied	CONFIRM	<a href="http://bugs.ghostscript.com">bugs.ghostscript.com</a>	Issue Tracking, Permissio
git.ghostscript.com Git - ghostpdl.git/commitdiff	CONFIRM	<a href="http://git.ghostscript.com">git.ghostscript.com</a>	Patch, Third Party Advise
Ghostscript CVE-2018-19134 Remote Code Execution Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	Third Party Advisory, VDI
git.ghostscript.com Git - ghostpdl.git/commitdiff		<a href="http://git.ghostscript.com">git.ghostscript.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**Free CVE JSON API** [cve.report/api](http://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)