



CVE-2008-5078

Published on: 12/19/2008 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:37 AM UTC

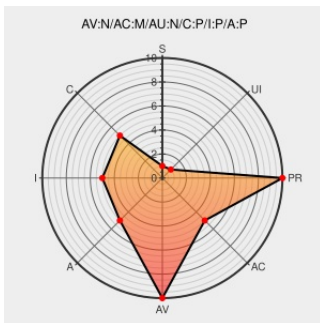
CVE-2008-5078

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Escript](#) from [Gnu](#) contain the following vulnerability:

Multiple buffer overflows in the (1) recognize_eps_file function (src/psgen.c) and (2) tilde_subst function (src/util.c) in GNU enscript 1.6.1, and possibly earlier, might allow remote attackers to execute arbitrary code via an epsf escape sequence with a long filename.

CVE-2008-5078 has been assigned by secalert@redhat.com to track the vulnerability

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

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](https://exchange.xforce.ibmcloud.com/text/html)
text/html

[XF enscript-recognize-tilde-bo\(47680\)](#)

Repository / Oval Repository

[oval.cisecurity.org](https://oval.cisecurity.org/text/html)
text/html

[OVAL oval:org.mitre.oval:def:11807](#)

GNU Enscript Buffer Overflows in Processing Special Escape Sequences Let Remote Users Execute Arbitrary Code - SecurityTracker

[www.securitytracker.com](https://www.securitytracker.com/text/html)
text/html

[SECTrack 1021401](#)

Bug 473958 – CVE-2008-5078 enscript: "epsf" special escape buffer overflows

[bugzilla.redhat.com](https://bugzilla.redhat.com/text/html)
text/html

[CONFIRM](#)
bugzilla.redhat.com/show_bug.cgi?id=473958

[security-announce] SUSE Security Summary Report: SUSE-SR:2009:005

[lists.opensuse.org](https://lists.opensuse.org/text/html)
text/html

[SUSE SUSE-SR:2009:005](#)

ASA-2008-504 (RHSA-2008-1021)	support.avaya.com text/html	 CONFIRM support.avaya.com/elmodocs2/security/ASA-2008-504.htm
Support	www.redhat.com text/html	 REDHAT RHSA-2008:1021
Red Hat update for enscript - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 33181

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Enscript	1.6.1	All	All	All
Application	Gnu	Enscript	1.6.1	All	All	All
cpe:2.3:a:gnu:enscript:1.6.1:****:***:						
cpe:2.3:a:gnu:enscript:1.6.1:****:***:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#)