



# CVE-2012-0035

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

## Summary

<b>CVE</b>	CVE-2012-0035
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2012-01-19 15:55:00 UTC
<b>Updated</b>	2018-12-07 11:29:00 UTC
<b>Description</b>	Untrusted search path vulnerability in EDE in CEDET before 1.0.1, as used in GNU Emacs before 23.4 and other products,

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	beta1	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	beta2	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	beta3	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre1	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre2	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre3	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre4	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre6	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre7	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	beta1	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	beta2	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	beta3	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre1	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre2	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre3	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre4	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre6	All	All

Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	1.0	pre7	All	All
Application	<a href="#">Eric M Ludlam</a>	<a href="#">Cedet</a>	All	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.0	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.5	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.6	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.7	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.2.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.3.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	22.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	22.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	22.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	23.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	23.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	23.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.0	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.5	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.6	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	20.7	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.2.1	All	All	All

Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.3.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	21.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	22.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	22.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	22.3	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	23.1	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	23.2	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	23.4	All	All	All
Application	<a href="#">Gnu</a>	<a href="#">Emacs</a>	All	All	All	All

## References

Reference	Source	Link	Tags
oss-security - CVE Request: CEDET/Emacs global-ede-mode file loading vulnerability	MLIST	<a href="https://openwall.com">openwall.com</a>	Patch
Support / Security / Advisories // MDVSA-2013:076   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>	
EDE: Privilege escalation (GLSA 201812-05) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>	
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Vendor
[SECURITY] Fedora 15 Update: emacs-23.3-8.fc15	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
[SECURITY] Fedora 16 Update: emacs-23.3-9.fc16	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CEDET / [CEDET-devel] Security flaw in EDE	MLIST	<a href="https://sourceforge.net">sourceforge.net</a>	
Security Advisory SA50801 - Ubuntu update for emacs23 - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>	
About Secunia Research   Flexera	SECUNIA	<a href="https://secunia.com">secunia.com</a>	Vendor
oss-security - Re: CVE Request: CEDET/Emacs global-ede-mode file loading vulnerability	MLIST	<a href="https://openwall.com">openwall.com</a>	
CEDET / [CEDET-devel] CEDET 1.0.1 available online	MLIST	<a href="https://sourceforge.net">sourceforge.net</a>	
USN-1586-1: Emacs vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	
Security flaw in EDE; new release plans	MLIST	<a href="https://lists.gnu.org">lists.gnu.org</a>	Patch
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[710288](#) Gentoo Linux EDE Privilege escalation Vulnerability (GLSA 201812-05)

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](#)**