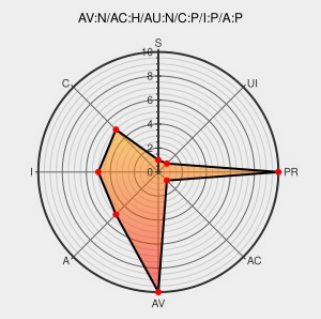
CVE-2003-1232

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

CVE-2003-1232

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Emacs from Gnu contain the following vulnerability:

Emacs 21.2.1 does not prompt or warn the user before executing Lisp code in the local variables section of a text file, which allows user-assisted attackers to execute arbitrary commands, as demonstrated using the mode-name variable.

CVE-2003-1232 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Advisories - Mandriva Linux OS	www.mandriva.com text/html	MANDRIVA MDKSA-2005:208
Emacs Local Variable Arbitrary Command Execution Vulnerability	cve.report (archive) text/html	BID 15375
#286183 - emacs21: Arbitrary code execution	bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=286183

execution when opening malicious file (local variables) - Debian Bug report logs		
Google Groups	groups.google.com text/html	MISC groups.google.com/group/gnu.emacs.bug/browse_frm/thread/9424ec1b2fdae321/c691a2da8904db0f?hl=en&lr=&ie=UTF-8&oe=UTF-8&rnum=1&prev=/groups%3Fq%3Dguninski%2Bemacs%26hl%3Den%26lr%3D%26ie%3DUTF-8%26oe%3DUTF-8%26selm%3Dmailman.763.1041357806.19936.bug-gnu-emacs%2540gnu.org%26rnum%3D1#c691a2da8904db0f
Secunia - Advisories - Mandriva update for emacs	web.archive.org text/html	SECUNIA 17496
[Full-Disclosure] emacs 21.3 fixes security bugs	Patch web.archive.org text/html Inactive Link Not Archived	MISC lists.grok.org.uk/pipermail/full-disclosure/2003-May/005089.html

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	Emacs	21.2.1	All	All	All
Application	Gnu	Emacs	21.2.1	All	All	All

cpe:2.3:a:gnu:emacs:21.2.1:*:*:*:*:*:*:*

cpe:2.3:a:gnu:emacs:21.2.1:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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