CVE-2008-1694

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-1694
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-04-22 04:41:00 UTC
Updated	2018-10-03 21:54:00 UTC
Description	vcdiff in Emacs 20.7 to 22.1.50, when used with SCCS, allows local users to overwrite arbitrary files via a symlink attack on

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Emacs	20.7	All	All	All
Application	Gnu	Emacs	21.1	All	All	All
Application	Gnu	Emacs	21.2	All	All	All
Application	Gnu	Emacs	21.3	All	All	All
Application	Gnu	Emacs	21.4	All	All	All
Application	Gnu	Emacs	20.7	All	All	All
Application	Gnu	Emacs	21.1	All	All	All
Application	Gnu	Emacs	21.2	All	All	All
Application	Gnu	Emacs	21.3	All	All	All
Application	Gnu	Emacs	21.4	All	All	All
Application	Gnu	Sccs	All	All	All	All
Application	Gnu	Sccs	All	All	All	All

References

Reference	Source	Link
XEmacs vcdiff Insecure Temporary Files - Advisories - Secunia	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ibm

Support / Security / Advisories / / MDVSA-2008:096 | Mandriva	MANDRIVA	www.mandriva.com
GNU Emacs Insecure Temporary File Creation Vulnerability	BID	www.securityfocus.co
Webmail - OVH	VUPEN	www.vupen.com
GNU Emacs vcdiff Unsafe Temporary File Lets Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	www.securitytracker.
Bug 208483 – CVE-2008-1694 emacs insecure /tmp file usage	CONFIRM	bugzilla.redhat.com
Gentoo Bug 216880 - app-editors/emacs vcdiff insecure temporary file creation (CVE-2008-1694)	CONFIRM	bugs.gentoo.org
GNU Emacs vcdiff Insecure Temporary Files - Advisories - Secunia	SECUNIA	secunia.com
USN-607-1: Emacs vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Ubuntu update for emacs - Advisories - Secunia	SECUNIA	secunia.com
Webmail - OVH	VUPEN	www.vupen.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2008-05-01	Joshua Bressers	Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.

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