



CVE-1999-0872

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

Summary

CVE	CVE-1999-0872
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	1999-08-25 04:00:00 UTC
Updated	2008-09-09 12:36:00 UTC
Description	Buffer overflow in Vixie cron allows local users to gain root access via a long MAILTO environment variable in a crontab file

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Caldera	Openlinux	2.2	All	All	All
Operating System	Caldera	Openlinux	2.2	All	All	All
Operating System	Debian	Debian Linux	2.1	All	All	All
Operating System	Debian	Debian Linux	2.2	All	All	All
Operating System	Debian	Debian Linux	2.1	All	All	All
Operating System	Debian	Debian Linux	2.2	All	All	All
Application	Paul Vixie	Vixie Cron	3.0_pl1	All	All	All
Application	Paul Vixie	Vixie Cron	3.0_pl1	All	All	All
Operating System	Redhat	Linux	4.0	All	All	All
Operating System	Redhat	Linux	4.1	All	All	All
Operating System	Redhat	Linux	4.2	All	All	All
Operating System	Redhat	Linux	5.0	All	All	All
Operating System	Redhat	Linux	5.1	All	All	All
Operating System	Redhat	Linux	5.2	All	i386	All
Operating System	Redhat	Linux	6.0	All	i386	All
Operating System	Redhat	Linux	4.0	All	All	All
Operating System	Redhat	Linux	4.1	All	All	All

Operating System	Redhat	Linux	4.2	All	All	All
Operating System	Redhat	Linux	5.0	All	All	All
Operating System	Redhat	Linux	5.1	All	All	All
Operating System	Redhat	Linux	5.2	All	i386	All
Operating System	Redhat	Linux	6.0	All	i386	All

References

Reference	Source	Link	Tags
Skyfull Mail Server MAIL FROM Buffer Overflow Vulnerability	BID	www.securityfocus.com	
Vixie Cron MAILTO Sendmail Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

© [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](#) 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