



CVE-2014-8504

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

Summary

CVE	CVE-2014-8504
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-09 23:59:00 UTC
Updated	2023-11-07 02:22:00 UTC
Description	Stack-based buffer overflow in the srec_scan function in bfd/srec.c in GNU binutils 2.24 and earlier allows remote attackers

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	19	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Application	Gnu	Binutils	All	All	All	All

References

Reference	Source	Link	Tags
Binutils: Multiple vulnerabilities (GLSA 201612-24) — Gentoo security	GENTOO	security.gentoo.org	
oss-security - Re: strings / libbfd crasher	MLIST	www.openwall.com	Mailing List, Third Party
oss-security - Re: Re: strings / libbfd crasher	MLIST	www.openwall.com	Exploit, Mailing List,
[SECURITY] Fedora 20 Update: cross-binutils-2.25-3.fc20	FEDORA	lists.fedoraproject.org	Third Party Advisory
sourceware.org Git - binutils-gdb.git/commit	CONFIRM	sourceware.org	Issue Tracking, Patc
Bug 17510 – strings: crash when given a truncated ELF	CONFIRM	sourceware.org	Exploit, Issue Tracki
sourceware.org Git - binutils-gdb.git/commit		sourceware.org	
[SECURITY] Fedora 21 Update: mingw-binutils-2.25-1.fc21	FEDORA	lists.fedoraproject.org	Third Party Advisory
Security Advisory SA62746 - SUSE update for binutils - Secunia	SECUNIA	secunia.com	Permissions Require
Support / Security / Advisories / / MDVSA-2015:029 Mandriva	MANDRIVA	www.mandriva.com	Broken Link
Bug 1162621 – CVE-2014-8504 binutils: stack overflow in the SREC parser	CONFIRM	bugzilla.redhat.com	Issue Tracking
[SECURITY] Fedora 21 Update: avr-binutils-2.24-4.fc21	FEDORA	lists.fedoraproject.org	Third Party Advisory
[SECURITY] Fedora 20 Update: mingw-binutils-2.24-5.fc20	FEDORA	lists.fedoraproject.org	Third Party Advisory
[SECURITY] Fedora 20 Update: avr-binutils-2.24-3.fc20	FEDORA	lists.fedoraproject.org	Third Party Advisory
USN-2496-1: GNU binutils vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Party Advisory
Security Advisory SA62241 - Debian update for binutils-mingw-w64 - Secunia	SECUNIA	secunia.com	Permissions Require
[SECURITY] Fedora 19 Update: avr-binutils-2.24-3.fc19	FEDORA	lists.fedoraproject.org	Third Party Advisory
binutils 'srec.c' Stack Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory
oss-security - Re: Re: strings / libbfd crasher	MLIST	www.openwall.com	Exploit, Mailing List,
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](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report