



CVE-2004-0400

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

Summary

CVE	CVE-2004-0400
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-07-07 04:00:00 UTC
Updated	2017-07-11 01:30:00 UTC
Description	Stack-based buffer overflow in Exim 4 before 4.33, when the headers_check_syntax option is enabled, allows remote attack

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	University Of Cambridge	Exim	All	All	All	All

References

Reference	Source	Link	Tags
Buffer overflows in exim, yet still exim much better than windows	MISC	www.guninski.com	Exploit, PoC
Debian -- Security Information -- DSA-502-1 exim-tls	DEBIAN	www.debian.org	Patch, Verified
Debian -- Security Information -- DSA-501-1 exim	DEBIAN	www.debian.org	Patch, Verified
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
[Full-Disclosure] Buffer overflows in exim, yet still exim much better than windows	FULLDISC	lists.grok.org.uk	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, NVD only

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)