CVE-2008-2719

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

Summary

CVE	CVE-2008-2719
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-16 23:41:00 UTC
Updated	2023-11-07 02:02:00 UTC
Description	Off-by-one error in the ppscan function (preproc.c) in Netwide Assembler (NASM) 2.02 allows context-dependent attackers

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nasm	Netwide Assembler	2.02	All	All	All
Application	Nasm	Netwide Assembler	2.02	All	All	All

References

Reference	Source	Link
Ubuntu update for nasm - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
The Netwide Assembler / Bugs / #349 nasm 2.02 triggers stack guard in glibc 2.7	CONFIRM	sourceforge.net
NASM Stack Overflow in Processing ASM Files Lets Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.securitytracke
USN-648-1: nasm vulnerability | Ubuntu	UBUNTU	www.ubuntu.com
NASM 'ppscan()' Off-By-One Buffer Overflow Vulnerability	BID	www.securityfocus
NASM "ppscan()" Off-By-One Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xforce.ib
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Public Git Hosting - nasm.git/commit	CONFIRM	repo.or.cz
The Netwide Assembler download | SourceForge.net	CONFIRM	sourceforge.net
oss-security - Re: CVE id request: nasm off-by-one	MLIST	www.openwall.com
Support / Security / Advisories / / MDVSA-2008:120 | Mandriva	MANDRIVA	www.mandriva.com

Public Git Hosting - nasm.git/commit		repo.or.cz
oss-security - CVE id request: nasm off-by-one	MLIST	www.openwall.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	2008-07-04	Mark J Cox	Not vulnerable. These issues did not affect the versions of NASM as shipped with Red Hat Ente

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 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.

Free CVE JSON API cve.report/api

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