



CVE-2013-6767

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2013-6767
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-12-20 22:55:06 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Stack-based buffer overflow in pepoly.dll in Quick Heal AntiVirus Pro 7.0.0.1 allows local users to execute arbitrary code or

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

AV:L/AC:L/Au:N/C:C/I:C/A:C

EPSS: 0.002570000 probability, percentile 0.490860000 (date 2026-05-15)

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Quickheal	Antivirus Pro	7.0.0.1	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References			
Reference	Source	Link	
Bugtraq: QuickHeal AntiVirus 7.0.0.1 - Stack Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	seclists.org	
osvdb.org/101130	af854a3a-2127-422b-91ae-364da2661108	osvdb.org	
403 Forbidden	af854a3a-2127-422b-91ae-364da2661108	www.vulneral	
QuickHeal AntiVirus 7.0.0.1 - Stack Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.exploit-c	
QuickHeal AntiVirus 'pepoly.dll' Module Local Stack Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.security	
QuickHeal AntiVirus 7.0.0.1 Stack Buffer Overflow ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108	packetstorms	
CVE Program record	CVE.ORG	www.cve.org	
NVD vulnerability detail	NVD	nvd.nist.gov	

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://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

Free CVE JSON API cve.report/api

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