



Published on: 05/02/2005 12:00:00 AM UTC

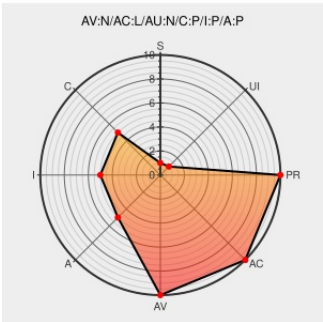
Last Modified on: 03/23/2021 11:27:24 PM UTC

CVE-2005-1391

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of **Pound** from **Apsis** contain the following vulnerability:

Buffer overflow in the `add_port` function in APSIS Pound 1.8.2 and earlier allows remote attackers to execute arbitrary code via a long Host HTTP header.

CVE-2005-1391 has been assigned by [M cve@mitre.org](mailto:m_cve@mitre.org) to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
#307852 - CAN-2005-1391: buffer overflow in add_port function - Debian Bug report logs	bugs.debian.org text/html	 MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=307852
APSYS Pound Remote Buffer Overflow Vulnerability	Patch cve.report (archive) text/html	 BID 13436
SecurityTracker.com Archives - Pound Buffer Overflow in add_port() Lets Remote Users Crash the Application	securitytracker.com text/html	 SECTrack 1013824
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2005-0437
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF pound-addport-bo(20316)
Debian -- Page not found	www.debian.org	 DEBIAN DSA-934

[Depreciated Link](#)[text/html](#)[Inactive Link](#)[Not Archived](#)[No Description Provided](#)[Vendor Advisory](#)[OSVDB 15963](#)[www.osvdb.org](#)[Inactive Link](#)[Not Archived](#)

Secunia - Advisories - SUSE update for bzip2/gaim/pound

[web.archive.org](#)[SECUNIA 15679](#)[text/html](#)

Secunia - Advisories - Gentoo update for pound

[web.archive.org](#)[SECUNIA 15202](#)[text/html](#)

Secunia - Advisories - Debian update for pound

[web.archive.org](#)[SECUNIA 18381](#)[text/html](#)

remote buffer overflow in pound 1.8.2 + question about Host header / Steven Van Acker

[Exploit](#)[web.archive.org](#)[text/html](#)[Inactive Link](#)[Not Archived](#)[MLIST \[pound_list\] 20050426 remote buffer overflow in pound 1.8.2 + question about Host header](#)

Gentoo Linux Documentation -- Pound: Buffer overflow vulnerability

[security.gentoo.org](#)[GENTOO GLSA-200504-29](#)[text/html](#)

Secunia - Advisories - Pound "add_port()" Function Buffer Overflow Vulnerability

[web.archive.org](#)[SECUNIA 15142](#)[text/html](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apsis	Pound	1.8.2	All	All	All
Application	Apsis	Pound	1.8.2	All	All	All
cpe:2.3:a:apsis:pound:1.8.2:*:*:*:*:*:						
cpe:2.3:a:apsis:pound:1.8.2:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

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](#)