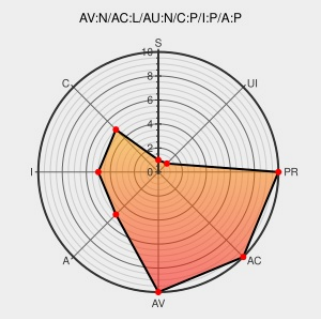
CVE-2005-1391

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 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
APSIS 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 www.osvdb.org Inactive Link Not Archived	OSVDB 15963
Secunia - Advisories - SUSE update for bzip2/gaim/pound	web.archive.org text/html	SECUNIA 15679
Secunia - Advisories - Gentoo update for pound	web.archive.org text/html	SECUNIA 15202
Secunia - Advisories - Debian update for pound	web.archive.org text/html	SECUNIA 18381
remote buffer overflow in pound 1.8.2 + question abotu 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 abotu Host header
Gentoo Linux Documentation -- Pound: Buffer overflow vulnerability	security.gentoo.org text/html	GENTOO GLSA-200504-29
Secunia - Advisories - Pound "add_port()" Function Buffer Overflow Vulnerability	web.archive.org text/html	SECUNIA 15142

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