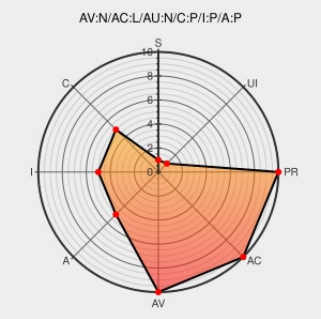
CVE-2004-2026

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:13 PM UTC

CVE-2004-2026

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pound from Apsis contain the following vulnerability:

Format string vulnerability in the logmsg function in svc.c for Pound 1.5 and earlier allows remote attackers to execute arbitrary code via format string specifiers in syslog messages.

CVE-2004-2026 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
Gentoo Linux Documentation -- Pound format string vulnerability	Patch, security.gentoo.org, text/html	GENTOO GLSA-200405-08
ANNOUNCE: Pound - reverse proxy and load balancer - v1.6 / Robert Segall	web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.apsis.ch/pound/pound_list/archive/2003/2003-12/1070234315000#1070234315000
Pound Format String Flaw in Syslog Processing Lets Remote Users Execute Arbitrary Code - SecurityTracker	securitytracker.com, text/html	SECTRACK 1010034
No Description Provided	Exploit, web.archive.org, text/html, Inactive Link, Not Archived	FULLDISC 20040507 Pound <=1.5 Remote Exploit (Format string bug)

Secunia - Advisories - Pound "logmsg()" Format String Vulnerability	Patch web.archive.org text/html	SECUNIA 11528
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 5746
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF pound-logmsg-format-string(16033)
APSIS Pound Remote Format String Vulnerability	Exploit Patch cve.report (archive) text/html	BID 10267

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	1.0	All	All	All
Application	Apsis	Pound	1.1	All	All	All
Application	Apsis	Pound	1.2	All	All	All
Application	Apsis	Pound	1.3	All	All	All
Application	Apsis	Pound	1.4	All	All	All
Application	Apsis	Pound	1.5	All	All	All
Application	Apsis	Pound	1.0	All	All	All
Application	Apsis	Pound	1.1	All	All	All
Application	Apsis	Pound	1.2	All	All	All
Application	Apsis	Pound	1.3	All	All	All
Application	Apsis	Pound	1.4	All	All	All
Application	Apsis	Pound	1.5	All	All	All

cpe:2.3:a:apsis:pound:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:apsis:pound:1.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→