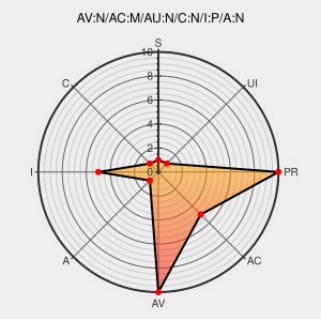
CVE-2005-3751

Published on: 11/22/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

CVE-2005-3751

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



Certain versions of Pound from Apsis contain the following vulnerability:

HTTP request smuggling vulnerability in Pound before 1.9.4 allows remote attackers to poison web caches, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with conflicting Content-length and Transfer-encoding headers.

CVE-2005-3751 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Announcement	web.archive.org, text/html, Inactive Link, Not Archived	SUSE SUSE-SR:2006:011
Gentoo Linux Documentation -- Pound: HTTP request smuggling	www.gentoo.org, text/html	GENTOO GLSA-200606-05
Debian -- Page not found	www.debian.org, Depreciated Link, text/html, Inactive Link, Not Archived	DEBIAN DSA-934
Secunia - Advisories - Debian update for pound	Vendor Advisory, web.archive.org, text/html	SECUNIA 18381
Secunia - Advisories - Pound HTTP Request	Vendor Advisory	SECUNIA 18367

Smuggling Vulnerability	web.archive.org text/html	
Gentoo update for pound - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20510
ANNOUNCE: Pound - reverse proxy and load balancer - v1.9.4 / Robert Segall	web.archive.org text/html Inactive Link Not Archived	MLIST [pound-list] 20051020 ANNOUNCE: Pound - reverse proxy and load balancer - v1.9.4
SUSE Updates for Multiple Packages - Advisories - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 20215

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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