

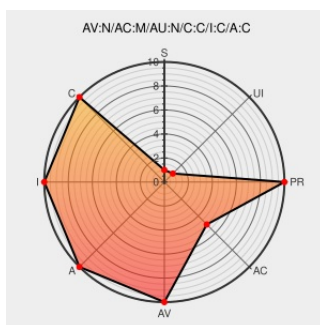


CVE-2011-4620

Published on: 12/30/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 03:06:56 AM UTC

CVE-2011-4620

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Plib](#) from [Steve J Baker](#) contain the following vulnerability:

Buffer overflow in the `ulSetError` function in `util/ulError.cxx` in `PLIB 1.8.5`, as used in `TORCS 1.3.1` and other products, allows user-assisted remote attackers to execute arbitrary code via vectors involving a long error message, as demonstrated by a crafted `acc` file for `TORCS`. NOTE: some of these details are obtained from third party

information.

CVE-2011-4620 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **9.3 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

Security Advisory SA51340 - SUSE update for plib - Secunia

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 51340](#)

PLIB: Buffer overflow vulnerability (GLSA 201606-16) — Gentoo security

[Third Party Advisory](#)
[security.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-201606-16](#)

TORCS 1.3.1 acc Buffer Overflow

[Exploit](#)
[Third Party Advisory](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 18258](#)

[security-announce] openSUSE-SU-2012:1506-1:
important: update for plib

Third Party Advisory
lists.opensuse.org
text/html

SUSE openSUSE-SU-2012:1506

oss-security - plib ulSetError() buffer overflow - CVE-2011-4620

openwall.com
text/html

MLIST [oss-security] 20111221 plib ulSetError() buffer overflow - CVE-2011-4620

No Description Provided

osvdb.org

OSVDB 77973

Inactive Link Not Archived

About Secunia Research | Flexera

Third Party Advisory
Vendor Advisory
secunia.com
Deprecated Link
text/plain

SECUNIA 47297

[security-announce] openSUSE-SU-2013:0146-1:
important: update for plib

Third Party Advisory
lists.opensuse.org
text/html

SUSE openSUSE-SU-2013:0146

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	Steve J Baker	Plib	1.8.5	All	All	All
Application	Steve J Baker	Plib	1.8.5	All	All	All
cpe:2.3:a:steve_j_baker:plib:1.8.5:*:*:*:*:*:						
cpe:2.3:a:steve_j_baker:plib:1.8.5:*:*:*:*:*:						

No vendor comments have been submitted for this CVE