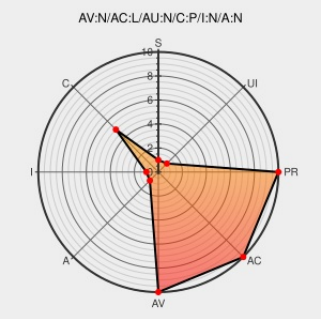
CVE-2005-1570

Published on: 05/14/2005 12:00:00 AM UTC

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

CVE-2005-1570

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



Certain versions of Bttlxeforum from Battleaxe Software contain the following vulnerability:

forum.asp in bttlxeForum 2.0 allows remote attackers to obtain full path information via a certain hex-encoded argument to the page parameter, possibly due to a SQL injection vulnerability.

CVE-2005-1570 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityTracker.com Archives - bttlxeForum Discloses Installation Path to Remote Users	Exploit, Vendor Advisory, securitytracker.com, text/html	SECTRACK 1013934

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)

Known Affected Configurations (CPE v2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Battleaxe Software	Bttlxeforum	2.0	All	All	All
Application	Battleaxe Software	Bttlxeforum	2.0	All	All	All

cpe:2.3:a:battleaxe_software:bttlxeforum:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:battleaxe_software:bttlxeforum:2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→