CVE-2001-0173

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2001-0173
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2001-05-03 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Buffer overflow in qDecoder library 5.08 and earlier, as used in CrazyWWWBoard, CrazySearch, and other CGI programs,

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:C/A:C

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:L/Au:N/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nobreak Technologies	Crazywwwboard	2000.0lepx	All	All	All

Application	Nobreak Technologies	Crazywwwboard	2000.0px	All	All	All
Application	Nobreak Technologies	Crazywwwboard	2000lepx	All	All	All
Application	Nobreak Technologies	Crazywwwboard	2000px	All	All	All
Application	Nobreak Technologies	Crazywwwboard	3.0.1	All	All	All
Application	Nobreak Technologies	Crazywwwboard	98	All	All	All
Application	Nobreak Technologies	Crazywwwboard	98pe	All	All	All
Application	Qdecoder	Qdecoder	4.0	All	All	All
Application	Qdecoder	Qdecoder	4.0.1	All	All	All
Application	Qdecoder	Qdecoder	4.3	All	All	All
Application	Qdecoder	Qdecoder	4.3.1	All	All	All
Application	Qdecoder	Qdecoder	5.0	All	All	All
Application	Qdecoder	Qdecoder	5.0.1	All	All	All
Application	Qdecoder	Qdecoder	5.0.2	All	All	All
Application	Qdecoder	Qdecoder	5.0.3	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
IBM X-Force Exchange
qDecoder Remote Buffer Overflow Vulnerability
Neohapsis Archives - Bugtraq - Nobreak Tecnologies CrazyWWWBoard Remote Buffer Overflow Vulnerability - From jhyou@CHONNAM.CH(
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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