



CVE-2006-0460

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

Summary

CVE	CVE-2006-0460
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-17 01:02:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Multiple buffer overflows in BomberClone before 0.11.6.2 allow remote attackers to execute arbitrary code via long error me

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

EPSS: 0.822180000 probability, percentile 0.992200000 (date 2026-04-16)

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Bomberclone	Bomberclone	0.1	All	All	All
Application	Bomberclone	Bomberclone	0.10.0	All	All	All
Application	Bomberclone	Bomberclone	0.11.3	All	All	All
Application	Bomberclone	Bomberclone	0.11.4	All	All	All
Application	Bomberclone	Bomberclone	0.11.5	All	All	All
Application	Bomberclone	Bomberclone	0.11.6	All	All	All
Application	Bomberclone	Bomberclone	0.2	All	All	All
Application	Bomberclone	Bomberclone	0.3	All	All	All
Application	Bomberclone	Bomberclone	0.4	All	All	All
Application	Bomberclone	Bomberclone	0.5	All	All	All
Application	Bomberclone	Bomberclone	0.6	All	All	All
Application	Bomberclone	Bomberclone	0.7	All	All	All
Application	Bomberclone	Bomberclone	0.8	All	All	All
Application	Bomberclone	Bomberclone	0.9.5	All	All	All
Application	Bomberclone	Bomberclone	0.9.6	All	All	All
Application	Bomberclone	Bomberclone	0.9.7	All	All	All
Application	Bomberclone	Bomberclone	0.9.8	All	All	All
Application	Bomberclone	Bomberclone	0.9.9	All	All	All

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

References			
Reference	Source		Link
BomberClone Error Message Buffer Overflow Vulnerability - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.cor
Debian -- Security Information -- DSA-997-1 bomberclone	af854a3a-2127-422b-91ae-364da2661108		www.debian
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108		exchange.x
BomberClone Error Messages Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108		www.securi
www.osvdb.org/23263	af854a3a-2127-422b-91ae-364da2661108		www.osvdb
Gentoo update for bomberclone - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.cor
Debian update for bomberclone - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108		secunia.cor
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108		www.vuper
Gentoo Linux Documentation -- BomberClone: Remote execution of arbitrary code	af854a3a-2127-422b-91ae-364da2661108		www.gento
CVE Program record	CVE.ORG		www.cve.or
NVD vulnerability detail	NVD		nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)