



CVE-2004-0724

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

Summary

CVE	CVE-2004-0724
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-07-27 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The Half-Life engine before July 7 2004 allows remote attackers to cause a denial of service (server or client crash) via an e

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Valve Software	Half-life	1.1.0.4	All	linux	All

Application	Valve Software	Half-life	1.1.0.4	All	windows	All
Application	Valve Software	Half-life	1.1.0.8	All	All	All
Application	Valve Software	Half-life	1.1.0.9	All	All	All
Application	Valve Software	Half-life	1.1.1.0	All	All	All
Application	Valve Software	Half-life Dedicated Server	3.1	All	All	All
Application	Valve Software	Half-life Dedicated Server	3.1.0.4	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.0.5	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.0.6	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.0.7	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.0.8	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.0.9	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.1.0	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.1.1c1	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.1.1d	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.1.1e	All	linux	All
Application	Valve Software	Half-life Dedicated Server	3.1.1.1e	All	win32	All
Application	Valve Software	Half-life Dedicated Server	3.1.3	All	All	All
Application	Valve Software	Half-life Dedicated Server	4.1.0.4	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.0.6	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.0.7	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.0.8	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.0.9	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.1.0	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.1.1c1	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.1.1d_beta	All	win32	All
Application	Valve Software	Half-life Dedicated Server	4.1.1.1e	All	linux	All
Application	Valve Software	Half-life Dedicated Server	4.1.1.1e	All	win32	All

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

References						
Reference	Source			Link		
'Remote crash of Half-Life servers and clients (versions before the' - MARC	af854a3a-2127-422b-91ae-364da2661108			marc.info		
Valve Software Half-Life Engine Remote Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108			www.securityfocus.com/bid/26611		
IBM X Force Exchange	af854a3a-2127-422b-91ae-364da2661108			exchange.xforce.ibmcloud.com/vulnerabilities/26611		

IBM X-Force Exchange	a1854a3a-2127-4220-91ae-3b40a2b61108	exchange.xforce.ibmcloud.com
CVE Program record	CVE.ORG	www.cve.org
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](#)