



CVE-2007-1047

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

Summary

CVE	CVE-2007-1047
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-21 17:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Unspecified vulnerability in Distributed Checksum Clearinghouse (DCC) before 1.3.51 allows remote attackers to delete or modify data on the server via the DCC web interface. The vulnerability exists in the DCC web interface, which is used to manage the DCC database. The vulnerability is caused by a lack of proper access control checks in the DCC web interface, which allows attackers to delete or modify data on the server via the DCC web interface. The vulnerability is a result of a design flaw in the DCC web interface, which does not properly restrict access to the DCC database. The vulnerability is a result of a design flaw in the DCC web interface, which does not properly restrict access to the DCC database.

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

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	Distributed Checksum Clearinghouse	Dcc	1.3	All	All	All

Application	Distributed Checksum Clearinghouse	Dcc	1.3.1	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.10	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.11	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.12	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.13	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.14	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.15	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.16	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.2	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.3	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.4	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.5	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.6	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.7	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.8	All	All	All
Application	Distributed Checksum Clearinghouse	Dcc	1.3.9	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
www.rhyolite.com/anti-spam/dcc/CHANGES	af854a3a-2127-422b-91ae-364da2661108	www.rhyolite.com
osvdb.org/33251	af854a3a-2127-422b-91ae-364da2661108	osvdb.org
DCC Unspecified Manipulation of Data - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108	secunia.com
Distributed Checksum Clearinghouse Unspecified Data Manipulation Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secunia.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vulncheck.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.

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