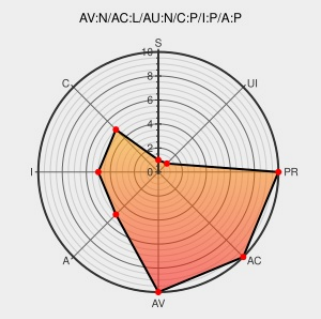
CVE-2002-1137

Published on: 10/11/2002 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1137

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



Certain versions of Data Engine from Microsoft contain the following vulnerability:

Buffer overflow in the Database Console Command (DBCC) that handles user inputs in Microsoft SQL Server 7.0 and 2000, including Microsoft Data Engine (MSDE) 1.0 and Microsoft Desktop Engine (MSDE) 2000, allows attackers to execute arbitrary code via a long SourceDB argument in a "non-SQL OLEDB data source" such as FoxPro, a variant of CAN-2002-0644.

CVE-2002-1137 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mssql-dbcc-bo-variant(10255)
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC N-003
Cisco Security Advisory: Microsoft SQL Server 2000 Vulnerabilities in Cisco Products - MS02-061	www.cisco.com text/html	CISCO 20030203 Microsoft SQL Server 2000 Vulnerabilities in Cisco Products - MS02-061
Microsoft Security Bulletin MS02-056 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS02-056

Microsoft SQL Server 7.0/2000 DBCC Buffer Overflow Vulnerability	Exploit Patch Vendor Advisory cve.report (archive) text/html	BID 5877
Home - Scan Associates	www.scan-associates.net text/plain	MISC www.scan-associates.net/papers/foxpro.txt

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)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Data Engine	1.0	All	All	All
Application	Microsoft	Data Engine	2000	All	All	All
Application	Microsoft	Data Engine	1.0	All	All	All
Application	Microsoft	Data Engine	2000	All	All	All
Application	Microsoft	Sql Server	2000	All	All	All
Application	Microsoft	Sql Server	2000	sp1	All	All
Application	Microsoft	Sql Server	2000	sp2	All	All
Application	Microsoft	Sql Server	7.0	All	All	All
Application	Microsoft	Sql Server	7.0	sp1	All	All
Application	Microsoft	Sql Server	7.0	sp2	All	All
Application	Microsoft	Sql Server	7.0	sp3	All	All
Application	Microsoft	Sql Server	7.0	sp4	All	All
Application	Microsoft	Sql Server	2000	All	All	All
Application	Microsoft	Sql Server	2000	sp1	All	All
Application	Microsoft	Sql Server	2000	sp2	All	All
Application	Microsoft	Sql Server	7.0	All	All	All
Application	Microsoft	Sql Server	7.0	sp1	All	All
Application	Microsoft	Sql Server	7.0	sp2	All	All
Application	Microsoft	Sql Server	7.0	sp3	All	All
Application	Microsoft	Sql Server	7.0	sp4	All	All

cpe:2.3:a:microsoft:data_engine:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:data_engine:2000:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:data_engine:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:data_engine:2000:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2000:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2000:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2000:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp4:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2000:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2000:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2000:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp1:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:7.0:sp4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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.

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