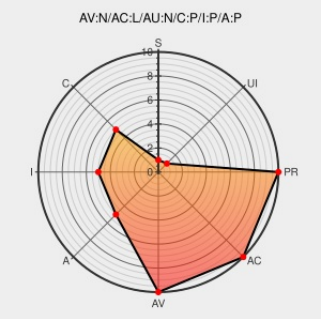
CVE-2002-1123

Published on: 09/24/2002 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:01 PM UTC

CVE-2002-1123

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



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

Buffer overflow in the authentication function for Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 allows remote attackers to execute arbitrary code via a long request to TCP port 1433, aka the "Hello" overflow.

CVE-2002-1123 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
'MS SQL Server Hello Overflow NASL script' - MARC	marc.info text/html	BUGTRAQ 20020807 MS SQL Server Hello Overflow NASL script
SecurityFocus HOME Mailing List: BugTraq	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20020806 SPIKE 2.5 and associated vulns
No Description Provided	web.archive.org text/html Inactive Link Not Archived	CIAC N-003
ISS X-Force Database: mssql-preauth-bo (9788): Microsoft SQL Server pre-authentication buffer overflow	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	XF mssql-preauth-bo(9788)
Microsoft SQL Server User Authentication Remote Buffer Overflow	cve.report (archive)	BID 5411

Vulnerability	text/html	
Microsoft Security Bulletin MS02-056 - Critical | Microsoft Docs	docs.microsoft.com text/html	MS MS02-056

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	2000	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	2000	All	All	All
Application	Microsoft	Sql Server	2000	sp1	All	All
Application	Microsoft	Sql Server	2000	sp2	All	All

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

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:2000:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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