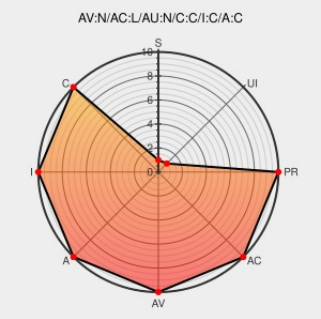
CVE-2002-1145

Published on: 10/21/2002 12:00:00 AM UTC

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

CVE-2002-1145

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



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

The xp_runwebtask stored procedure in the Web Tasks component of Microsoft SQL Server 7.0 and 2000, Microsoft Data Engine (MSDE) 1.0, and Microsoft Desktop Engine (MSDE) 2000 can be executed by PUBLIC, which allows an attacker to gain privileges by updating a webtask that is owned by the database owner through the msdb.dbo.mswebtasks table, which does not have strong permissions.

CVE-2002-1145 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
'Microsoft SQL Server Webtasks privilege upgrade (#NISR17102002)' - MARC	marc.info, text/html	NTBUGTRAQ 20021017 Microsoft SQL Server Webtasks privilege upgrade (#NISR17102002)
ISS X-Force Database: mssql-webtask-gain-privileges (10388): Microsoft SQL Server Web tasks could allow elevated privileges	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	XF mssql-webtask-gain-privileges(10388)
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 MS02-061 - Critical | Microsoft Docs	docs.microsoft.com	MS MS02-061

	text/html	
nextgenss.com - This website is for sale! - nextgenss Resources and Information.	www.nextgenss.com text/plain	MISC www.nextgenss.com/advisories/mssql-webtasks.txt
'Microsoft SQL Server Webtasks privilege upgrade (#NISR17102002)' - MARC	marc.info text/html	BUGTRAQ 20021017 Microsoft SQL Server Webtasks privilege upgrade (#NISR17102002)
Microsoft SQL Server Web Task Stored Procedure Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 5980

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→