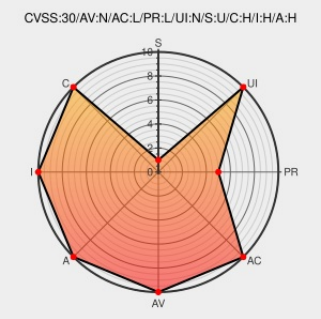
CVE-2016-7254

Published on: 11/10/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:07 PM UTC

CVE-2016-7254

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



Certain versions of Sql Server from Microsoft contain the following vulnerability:

Microsoft SQL Server 2012 SP2 and 2012 SP3 does not properly perform a cast of an unspecified pointer, which allows remote authenticated users to gain privileges via unknown vectors, aka "SQL RDBMS Engine Elevation of Privilege Vulnerability."

CVE-2016-7254 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Microsoft Security Bulletin MS16-136 - Important | Microsoft Docs	docs.microsoft.com, text/html	MS MS16-136
Microsoft SQL Server Flaws Let Remote Users Conduct Cross-Site Scripting Attacks and Remote Authenticated Users Obtain Potentially Sensitive Information and Gain Elevated Privileges -	www.securitytracker.com, text/html	SECTRACK

SecurityTracker		1037250
Microsoft SQL Server CVE-2016-7254 Privilege Escalation Vulnerability	cve.report (archive) text/html	BID 94061

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	Sql Server	2012	sp2	All	All
Application	Microsoft	Sql Server	2012	sp3	All	All
Application	Microsoft	Sql Server	2012	sp2	All	All
Application	Microsoft	Sql Server	2012	sp3	All	All

cpe:2.3:a:microsoft:sql_server:2012:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2012:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2012:sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2012:sp3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→