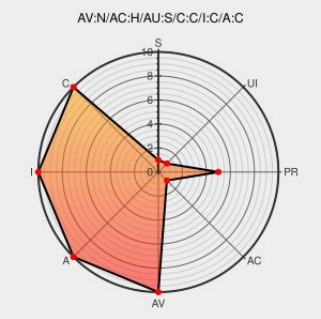
CVE-2015-1762

Published on: 07/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1762

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



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

Microsoft SQL Server 2008 SP3 and SP4, 2008 R2 SP2 and SP3, 2012 SP1 and SP2, and 2014, when transactional replication is configured, does not prevent use of uninitialized memory in unspecified function calls, which allows remote authenticated users to execute arbitrary code by leveraging certain permissions and making a crafted query, as demonstrated by the VIEW SERVER STATE permission, aka "SQL Server Remote Code Execution Vulnerability."

CVE-2015-1762 has been assigned by secure@microsoft.com to track the vulnerability

CVSS2 Score: 7.1 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Microsoft Security Bulletin MS15-058 - Important | Microsoft Docs	docs.microsoft.com text/html	MS MS15-058
Microsoft SQL Server Bugs Let Remote Authenticated Users Gain Privilege Escalation and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1032893

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	2008	r2_sp2	All	All
Application	Microsoft	Sql Server	2008	r2_sp3	All	All
Application	Microsoft	Sql Server	2008	sp3	All	All
Application	Microsoft	Sql Server	2008	sp4	All	All
Application	Microsoft	Sql Server	2012	sp1	All	All
Application	Microsoft	Sql Server	2012	sp2	All	All
Application	Microsoft	Sql Server	2014	All	All	All
Application	Microsoft	Sql Server	2008	r2_sp2	All	All
Application	Microsoft	Sql Server	2008	r2_sp3	All	All
Application	Microsoft	Sql Server	2008	sp3	All	All
Application	Microsoft	Sql Server	2008	sp4	All	All
Application	Microsoft	Sql Server	2012	sp1	All	All
Application	Microsoft	Sql Server	2012	sp2	All	All
Application	Microsoft	Sql Server	2014	All	All	All

cpe:2.3:a:microsoft:sql_server:2008:r2_sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:r2_sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:sp4:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2012:sp1:*:*:*:*:*:*:

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

cpe:2.3:a:microsoft:sql_server:2014:*:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:r2_sp2:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:r2_sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:sp3:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2008:sp4:*:*:*:*:*:*:

cpe:2.3:a:microsoft:sql_server:2012:sp1:*:*:*:*:*:*:

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

cpe:2.3:a:microsoft:sql_server:2014:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→