



CVE-2018-8232

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-8232
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-11 00:29:00 UTC
Updated	2018-09-06 15:21:00 UTC
Description	A Tampering vulnerability exists when Microsoft Macro Assembler improperly validates code, aka "Microsoft Macro Assembl

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Visual Studio 2017	-	All	All	All
Application	Microsoft	Visual Studio 2017	15.7.5	All	All	All
Application	Microsoft	Visual Studio 2017	15.8	All	All	All
Application	Microsoft	Visual Studio 2017	-	All	All	All
Application	Microsoft	Visual Studio 2017	15.7.5	All	All	All
Application	Microsoft	Visual Studio 2017	15.8	All	All	All

References

Reference	Source
portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8232	CONFIRM
Microsoft Macro Assembler CVE-2018-8232 Security Bypass Vulnerability	BID
Microsoft Visual Studio Flaw in Microsoft Macro Assembler Lets Local Users Modify Data on the Target System - SecurityTracker	SECTRA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

91810 Microsoft Visual Studio 2017 Security Update for July 2018

© [CVE.report](#) 2026 |

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 registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)