



# CVE-2018-0986

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-0986
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-04-04 17:29:00 UTC
<b>Updated</b>	2021-09-09 13:34:00 UTC
<b>Description</b>	A remote code execution vulnerability exists when the Microsoft Malware Protection Engine does not properly scan a speci

## Risk And Classification

**Problem Types:** CWE-787


## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2013	-	All	All
Application	Microsoft	Exchange Server	2016	-	All	All
Application	Microsoft	Exchange Server	2013	-	All	All
Application	Microsoft	Exchange Server	2016	-	All	All
Application	Microsoft	Forefront Endpoint Protection 2010	-	All	All	All
Application	Microsoft	Forefront Endpoint Protection 2010	-	All	All	All
Application	Microsoft	Intune Endpoint Protection	-	All	All	All
Application	Microsoft	Intune Endpoint Protection	-	All	All	All
Application	Microsoft	Security Essentials	-	All	All	All
Application	Microsoft	Security Essentials	-	All	All	All
Application	Microsoft	System Center 2012 Endpoint Protection	All	All	All	All
Application	Microsoft	System Center 2012 Endpoint Protection	All	All	All	All
Application	Microsoft	System Center 2012 R2 Endpoint Protection	All	All	All	All
Application	Microsoft	System Center 2012 R2 Endpoint Protection	All	All	All	All
Application	Microsoft	System Center Endpoint Protection	All	All	All	All
Application	Microsoft	System Center Endpoint Protection	2012	-	All	All
Application	Microsoft	System Center Endpoint Protection	2012	r2	All	All

Application	Microsoft	System Center Endpoint Protection	All	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1511	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Operating System	Microsoft	Windows 8.1	All	All	All	All
Application	Microsoft	Windows Defender	-	All	All	All
Application	Microsoft	Windows Defender	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Rt 8.1	All	All	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	All	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	All	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	All	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All

## References

Reference	Source
<a href="https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0986">portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0986</a>	CONF
Microsoft Windows Defender File Processing Memory Corruption Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECT
Microsoft Windows Defender - 'mpengine.dll' Memory Corruption - Windows dos Exploit	EXPL
Microsoft Windows Defender File Processing Memory Corruption Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	CONF

Microsoft Malware Protection Engine CVE-2018-0986 Remote Code Execution Vulnerability	BID
CVE Program record	CVE.C
NVD vulnerability detail	NVD
	
<p>No vendor comments have been submitted for this CVE.</p>	
<p>There are currently no legacy QID mappings associated with this CVE.</p>	

© [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](#).

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