



# CVE-2017-8540

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

## Summary

<b>CVE</b>	CVE-2017-8540
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-05-26 20:29:00 UTC
<b>Updated</b>	2017-08-13 01:29:00 UTC
<b>Description</b>	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Ser

## Risk And Classification

**EPSS:** 0.846130000 probability, percentile 0.993260000 (date 2026-04-02)

**CISA KEV:** Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

**Problem Types:** CWE-119

## CISA Known Exploited Vulnerability

<b>Vendor</b>	Microsoft
<b>Product</b>	Malware Protection Engine
<b>Name</b>	Microsoft Malware Protection Engine Improper Restriction of Operations Vulnerability
<b>Required Action</b>	Apply updates per vendor instructions.
<b>Notes</b>	<a href="https://nvd.nist.gov/vuln/detail/CVE-2017-8540">https://nvd.nist.gov/vuln/detail/CVE-2017-8540</a>

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2013	All	All	All
Application	Microsoft	Exchange Server	2016	All	All	All
Application	Microsoft	Exchange Server	2013	All	All	All
Application	Microsoft	Exchange Server	2016	All	All	All
Application	Microsoft	Forefront Security	-	All	All	All
Application	Microsoft	Forefront Security	-	All	All	All
Application	Microsoft	Malware Protection Engine	All	All	All	All
Operating System	Microsoft	Windows 10	All	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	All	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 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
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All

## References

### Reference

{{windowTitle}}

Microsoft MsMpEng - Remote Use-After-Free Due to Design Issue in GC Engine - Windows dos Exploit

Microsoft Malware Protection Engine CVE-2017-8540 Remote Code Execution Vulnerability

Microsoft Malware Protection Engine File Processing Flaws Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker

CVE Program record

NVD vulnerability detail

CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)**