CVE-2017-8540

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-8540
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-26 20:29:00 UTC
Updated	2017-08-13 01:29:00 UTC
Description	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

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

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 and Source URL Uptime Status status.cve.report