



CVE-2017-0005

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|---|
| CVE | CVE-2017-0005 |
| State | PUBLIC |
| Assigner | secure@microsoft.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2017-03-17 00:59:00 UTC |
| Updated | 2019-10-03 00:03:00 UTC |
| Description | The Graphics Device Interface (GDI) in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 |

Risk And Classification

EPSS: 0.080100000 probability, percentile 0.920700000 (date 2026-04-01)

CISA KEV: Listed on 2022-05-24; due 2022-06-14; ransomware use Unknown

Problem Types: CWE-119

CISA Known Exploited Vulnerability

| | |
|------------------------|---|
| Vendor | Microsoft |
| Product | Windows |
| Name | Microsoft Windows Graphics Device Interface (GDI) Privilege Escalation Vulnerability |
| Required Action | Apply updates per vendor instructions. |
| Notes | https://nvd.nist.gov/vuln/detail/CVE-2017-0005 |

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|----------------------------|---------|--------|---------|----------|
| 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 | - | 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 7 | All | sp1 | All | All |
| Operating System | Microsoft | Windows 7 | All | sp1 | All | All |

| | | | | | | |
|------------------|-----------|---------------------|-----|-----|-----|-----|
| Operating System | Microsoft | Windows 8.1 | All | All | All | All |
| Operating System | Microsoft | Windows 8.1 | All | 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 | All | sp2 | All | All |
| Operating System | Microsoft | Windows Server 2008 | r2 | sp1 | All | All |
| Operating System | Microsoft | Windows Server 2008 | All | 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 Vista | All | sp2 | All | All |
| Operating System | Microsoft | Windows Vista | All | sp2 | All | All |

References

Reference

Detecting and mitigating elevation-of-privilege exploit for CVE-2017-0005 – Microsoft Malware Protection Center Blog

portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0005

Microsoft GDI+ Multiple Bugs Let Remote Users Obtain Potentially Sensitive Information and Execute Arbitrary Code and Let Local Users Gain Administrative Privileges

Microsoft Windows Graphics CVE-2017-0005 Local Privilege Escalation Vulnerability

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