# CVE-2017-0101

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-0101 |
| **State** | PUBLISHED |
| **Assigner** | microsoft |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-03-17 00:59:02 UTC |
| **Updated** | 2026-04-22 13:49:57 UTC |
| **Description** | The kernel-mode drivers in Transaction Manager in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2; Win |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from nvd@nist.gov

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

**EPSS:** 0.722640000 probability, percentile 0.987650000 (date 2026-04-26)

**CISA KEV:** Listed on 2022-03-15; due 2022-04-05; ransomware use Known

**Problem Types:** CWE-119 | Elevation of Privilege | CWE-119 CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 3.1 | nvd@nist.gov | Primary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | ADP | DECLARED | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 3.1 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 7.8 | HIGH | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H |
| 2.0 | nvd@nist.gov | Primary | 6.8 | | AV:N/AC:M/Au:N/C:P/I:P/A:P |

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | Microsoft |
| **Product** | Windows |
| **Name** | Microsoft Windows Transaction Manager Privilege Escalation Vulnerability |
| **Required Action** | Apply updates per vendor instructions. |
| **Notes** | https://nvd.nist.gov/vuln/detail/CVE-2017-0101 |

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Microsoft | Windows 7 | - | sp1 | All | All |
| Operating System | Microsoft | Windows Server 2008 | - | sp2 | All | All |
| Operating System | Microsoft | Windows Vista | - | sp2 | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version |
|---|---|---|---|

| | | | |
|---|---|---|---|
| CNA | Microsoft Corporation | Windows | affected The kernel-mode drivers in Transaction Manager in Microsoft Windows Vista SP2; Win |

## References

| Reference | Source |
|---|---|
| Microsoft Windows Kernel (7 x86) - Local Privilege Escalation (MS17-017) - Windows_x86 local Exploit | af854a3a-2127-422b-91ae-364da26 |
| Microsoft Windows CVE-2017-0101 Local Privilege Escalation Vulnerability | af854a3a-2127-422b-91ae-364da26 |
| Windows Kernel Bugs Let Local Users Gain Elevated Privileges - SecurityTracker | af854a3a-2127-422b-91ae-364da26 |
| www.cisa.gov/known-exploited-vulnerabilities-catalog | 134c704f-9b21-4f2e-91b3-4a46735 |
| Security Update Guide - Microsoft Security Response Center | af854a3a-2127-422b-91ae-364da26 |
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |
| CISA Known Exploited Vulnerabilities catalog | CISA |

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

| Source | Time | Event |
|---|---|---|
| ADP | 2022-03-15T00:00:00.000Z | CVE-2017-0101 added to CISA KEV |

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



**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**