# CVE-2012-1854

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2012-1854 |
| **State** | PUBLISHED |
| **Assigner** | microsoft |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2012-07-10 21:55:05 UTC |
| **Updated** | 2026-04-13 18:16:24 UTC |
| **Description** | Untrusted search path vulnerability in VBE6.dll in Microsoft Office 2003 SP3, 2007 SP2 and SP3, and 2010 Gold and SP1; |

## Risk And Classification

**Primary CVSS:** v3.1 7.8 HIGH from ADP

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

**EPSS:** 0.100700000 probability, percentile 0.931010000 (date 2026-04-18)

**CISA KEV:** Listed on 2026-04-13; due 2026-04-27; ransomware use Unknown

**Problem Types:** NVD-CWE-Other | CWE-426 | n/a | CWE-426 CWE-426 Untrusted Search Path

| Version | Source | Type | Score | Severity | Vector |
|---|---|---|---|---|---|
| 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 | 6.9 | | AV:L/AC:M/Au:N/C:C/I:C/A:C |

## 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

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## CISA Known Exploited Vulnerability

| | |
|---|---|
| **Vendor** | Microsoft |
| **Product** | Visual Basic for Applications (VBA) |
| **Name** | Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability |
| **Required Action** | Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable. |
| **Notes** | https://learn.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-046 ; https://nvd.nist.gov/vuln/detail/CVE-2012-1854 |

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Microsoft | Office | 2003 | sp3 | All | All |
| Application | Microsoft | Office | 2007 | sp2 | All | All |
| Application | Microsoft | Office | 2007 | sp3 | All | All |
| Application | Microsoft | Office | 2010 | All | x86 | All |
| Application | Microsoft | Office | 2010 | sp1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Microsoft | Office | 2010 | sp1 | x64 | All |
| Application | Microsoft | Office | 2010 | sp1 | x86 | All |
| Application | Microsoft | Visual Basic For Applications | All | All | All | All |
| Application | Microsoft | Visual Basic For Applications Sdk | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| learn.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-046 | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | learn.microsoft.c |
| Repository / Oval Repository | af854a3a-2127-422b-91ae-364da2661108 | oval.cisecurity.or |
| US-CERT Alert TA12-192A - Microsoft Updates for Multiple Vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | www.us-cert.gov |
| Microsoft Security Bulletin MS12-046 - Important \| Microsoft Docs | af854a3a-2127-422b-91ae-364da2661108 | docs.microsoft.c |
| www.cisa.gov/known-exploited-vulnerabilities-catalog | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | www.cisa.gov |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |
| CISA Known Exploited Vulnerabilities catalog | CISA | www.cisa.gov |

No vendor comments have been submitted for this CVE.

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