



CVE-2014-2817

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-2817
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-12 21:55:07 UTC
Updated	2026-04-22 13:54:11 UTC
Description	Microsoft Internet Explorer 6 through 11 allows remote attackers to gain privileges via a crafted web site, aka "Internet Explorer 6 through 11 Remote Code Execution Vulnerability"

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.290610000 probability, percentile 0.966220000 (date 2026-05-13)

CISA KEV: Listed on 2022-05-25; due 2022-06-15; ransomware use Unknown

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/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

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/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	Internet Explorer
Name	Microsoft Internet Explorer Privilege Escalation Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2014-2817

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Internet Explorer	6	All	All	All
Application	Microsoft	Internet Explorer	7	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CVE-2014-2817	Microsoft	Internet Explorer	6, 7	Windows Server 2003

CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
Microsoft Internet Explorer CVE-2014-2817 Remote Privilege Escalation Vulnerability			af854a3a-2127-422b-91ae-364da26	
www.cisa.gov/known-exploited-vulnerabilities-catalog			134c704f-9b21-4f2e-91b3-4a467353	
Microsoft Security Bulletin MS14-051 - Critical Microsoft Docs			af854a3a-2127-422b-91ae-364da26	
Microsoft Internet Explorer Mulitple Flaws Let Remote Users Execute Arbitrary Code - SecurityTracker			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	2022-05-25T00:00:00.000Z	CVE-2014-2817 added to CISA KEV		
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)