



CVE-2013-1347

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2013-1347
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-05-05 11:07:00 UTC
Updated	2026-04-22 16:45:05 UTC
Description	Microsoft Internet Explorer 8 does not properly handle objects in memory, which allows remote attackers to execute arbitrar

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: 0.877080000 probability, percentile 0.994740000 (date 2026-04-24)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Unknown

Problem Types: CWE-416 | n/a | CWE-416 CWE-416 Use After Free

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

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

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Internet Explorer
Name	Microsoft Internet Explorer Remote Code Execution Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2013-1347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Internet Explorer	8	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	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 Vista	-	sp2	All	All

Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Microsoft Security Bulletin MS13-038 - Critical Microsoft Docs	af854a3a-2127-422b-91ae-36
Microsoft Updates for Multiple Vulnerabilities US-CERT	af854a3a-2127-422b-91ae-36
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a
Repository / Oval Repository	af854a3a-2127-422b-91ae-36
Microsoft Internet Explorer CGenericElement Object Use-After-Free Vulnerability	af854a3a-2127-422b-91ae-36
Microsoft Security Advisory (2847140): Vulnerability in Internet Explorer Could Allow Remote Code Execution	af854a3a-2127-422b-91ae-36
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	2022-03-03T00:00:00.000Z	CVE-2013-1347 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](#)