CVE-2010-0249

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

Summary

CVE	CVE-2010-0249
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-01-15 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Use-after-free vulnerability in Microsoft Internet Explorer 6, 6 SP1, 7, and 8 on Windows 2000 SP4; Windows XP SP2 and S

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

Problem Types: CWE-416 | n/a

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
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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Internet Explorer	5.0.1	sp4	All	All
Application	Microsoft	Internet Explorer	6	-	All	All
Application	Microsoft	Internet Explorer	6	sp1	All	All
Application	Microsoft	Internet Explorer	7.0	All	All	All
Operating System	Microsoft	Windows 2000	-	sp4	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Server 2003	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	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
Internet Explorer Aurora Exploit	af854a3a-

Security Advisory 979352 Released - The Microsoft Security Response Center (MSRC) - Site Home - TechNet Blogs	af854a3a-
New IE hole exploited in attacks on U.S. firms | InSecurity Complex - CNET News	af854a3a-
IBM X-Force Exchange	af854a3a-
SecurityTracker.com Archives - Microsoft Internet Explorer Invalid Pointer Reference Lets Remote Users Execute Arbitrary Code	af854a3a-
Microsoft Security Advisory (979352): Vulnerability in Internet Explorer Could Allow Remote Code Execution	af854a3a-
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-
US-CERT Vulnerability Note VU#492515	af854a3a-
Microsoft Security Advisory: Vulnerability in Internet Explorer could allow remote code execution	af854a3a-
US-CERT Technical Cyber Security Alert TA10-055A -- Malicious Activity Associated with "Aurora" Internet Explorer Exploit	af854a3a-
Microsoft Security Bulletin MS10-002 - Critical | Microsoft Docs	af854a3a-
Repository / Oval Repository	af854a3a-
Internet Explorer CVE-2010-0249 'srcElement()' Remote Code Execution Vulnerability	af854a3a-
osvdb.org/61697	af854a3a-
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 registred 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**