CVE-2012-4969

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

Summary

CVE	CVE-2012-4969
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-18 10:39:14 UTC
Updated	2026-04-21 18:37:37 UTC
Description	Use-after-free vulnerability in the CMshtmlEd::Exec function in mshtml.dll in Microsoft Internet Explorer 6 through 9 allows r

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from nvd@nist.gov

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

EPSS: 0.917770000 probability, percentile 0.996950000 (date 2026-05-07)

CISA KEV: Listed on 2022-06-08; due 2022-06-22; 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	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/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

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/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 Use-After-Free Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2012-4969

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
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	-	sp3	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Zero-Day Season Is Really Not Over Yet	af854a3a-2127-422b-9
US-CERT Alert TA12-255A - Microsoft Updates for Multiple Vulnerabilities	af854a3a-2127-422b-9
US-CERT Alert TA12-265A - Microsoft Releases Patch for Internet Explorer Exploit	af854a3a-2127-422b-9
New Internet Explorer Zero-Day Being Exploited in the Wild | SecurityWeek.Com	af854a3a-2127-422b-9
Microsoft Security Advisory (2757760): Vulnerability in Internet Explorer Could Allow Remote Code Execution	af854a3a-2127-422b-9
US-CERT Alert TA12-262A - Microsoft Security Advisory for Internet Explorer Exploit	af854a3a-2127-422b-9
IE execCommand fuction Use after free Vulnerability 0day en	af854a3a-2127-422b-9
/modules/exploits/windows/browser/ie_execcommand_uaf.rb - Metasploit Framework - Metasploit Redmine Interface	af854a3a-2127-422b-9
Repository / Oval Repository	af854a3a-2127-422b-9
US-CERT Vulnerability Note VU#480095 - Microsoft Internet Explorer 6/7/8/9 contain a use-after-free vulnerability	af854a3a-2127-422b-9
Microsoft Internet Explorer execCommand Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-9
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-9
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	2022-06-08T00:00:00.000Z	CVE-2012-4969 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**