CVE-2012-4792

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

Summary

CVE	CVE-2012-4792
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-12-30 18:55:00 UTC
Updated	2023-12-07 18:38:00 UTC
Description	Use-after-free vulnerability in Microsoft Internet Explorer 6 through 8 allows remote attackers to execute arbitrary code via a

Risk And Classification

EPSS: 0.914290000 probability, percentile 0.996620000 (date 2026-04-06)

CISA KEV: Listed on 2024-07-23; due 2024-08-13; ransomware use Unknown

Problem Types: CWE-399

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Internet Explorer
Name	Microsoft Internet Explorer Use-After-Free Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://learn.microsoft.com/en-us/lifecycle/products/internet-explorer-11; https://nvd.nist.gov/vuln/detail/CVE-2012-4792

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
Application	Microsoft	Internet Explorer	8	All	All	All
Application	Microsoft	Internet Explorer	6	All	All	All
Application	Microsoft	Internet Explorer	7	All	All	All
Application	Microsoft	Internet Explorer	8	All	All	All
Operating System	Microsoft	Windows 7	-	All	All	All

Operating System	Microsoft	Windows 7	-	sp1	x64	All
Operating System	Microsoft	Windows 7	-	sp1	x86	All
Operating System	Microsoft	Windows 7	-	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	x64	All
Operating System	Microsoft	Windows 7	-	sp1	x86	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2003	All	sp2	All	All
Operating System	Microsoft	Windows Server 2008	All	r2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	itanium	All
Operating System	Microsoft	Windows Server 2008	All	r2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x64	All
Operating System	Microsoft	Windows Server 2008	All	sp2	x86	All
Operating System	Microsoft	Windows Server 2008	-	sp2	itanium	All
Operating System	Microsoft	Windows Vista	All	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Vista	All	sp2	x64	All
Operating System	Microsoft	Windows Vista	-	sp2	All	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	All	sp3	All	All
Operating System	Microsoft	Windows Xp	-	sp2	x64	All

References

Reference
Malware Intelligence Lab from FireEye - Research & Analysis of Zero-Day & Advanced Targeted Threats:CFR Watering Hole Attack Details
Attack and IE 0day Informations Used Against Council on Foreign Relations
Microsoft "Fix it" available for Internet Explorer 6, 7, and 8 - Security Research & Defense - Site Home - TechNet Blogs
Microsoft Internet Explorer CDwnBindInfo Object Use-After-Free ≈ Packet Storm
Just another water hole campaign using an Internet Explorer 0day - Alienvault Labs
Microsoft Updates for Multiple Vulnerabilities | US-CERT
Repository / Oval Repository

Microsoft Security Bulletin MS13-008 - Critical | Microsoft Docs
US-CERT Alert TA13-015A - Microsoft Releases Update for Internet Explorer Vulnerability CVE-2012-4792
metasploit-framework/modules/exploits/windows/browser/ie_cbutton_uaf.rb at master · rapid7/metasploit-framework · GitHub
US-CERT Vulnerability Note VU#154201 - Microsoft Internet Explorer CDwnBindInfo use-after-free vulnerability
New vulnerability affecting Internet Explorer 8 users - Security Research & Defense - Site Home - TechNet Blogs
Microsoft Security Advisory (2794220): Vulnerability in Internet Explorer Could Allow Remote Code Execution
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

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