CVE-2010-3971

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

Summary

CVE	CVE-2010-3971
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-12-22 21:00:00 UTC
Updated	2021-07-23 15:12:00 UTC
Description	Use-after-free vulnerability in the CSharedStyleSheet::Notify function in the Cascading Style Sheets (CSS) parser in mshtm

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Ie	7	All	All	All
Application	Microsoft	Ie	8	All	All	All
Application	Microsoft	Ie	7	All	All	All
Application	Microsoft	Ie	8	All	All	All
Application	Microsoft	Internet Explorer	7	All	All	All
Application	Microsoft	Internet Explorer	8	All	All	All

References

Reference	S
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	V
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	V
Microsoft Internet Explorer CSS Parsing Remote Memory Corruption Vulnerability	B
US-CERT Vulnerability Note VU#634956	C
Internet Explorer 8 CSS Parser Denial of Service	E
Assessing the risk of public issues currently being tracked by the MSRC - Security Research & Defense - Site Home - TechNet Blogs	M
Internet Explorer 8 CSS Parser Exploit	E
Full Disclosure: IE CSS parser dos bug	F

Microsoft Internet Explorer Recursive CSS Import Memory Corruption Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	S
Microsoft Security Bulletin MS11-003 - Critical | Microsoft Docs	M
IE8 CSS解析拒绝服务漏洞 | WooYun-2010-00885 | WooYun.org	M
Your request has been blocked. This could be due to several reasons.	M
When A DoS Isn't A DoS | BreakingPoint	M
ASA-2011-024 (2482017)	C
Repository / Oval Repository	O
Internet Explorer CSS Import Rule Processing Use-After-Free Vulnerability - Advisories - Community	S
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

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**