



CVE-2008-1441

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-1441
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-12 02:32:00 UTC
Updated	2018-10-12 21:45:00 UTC
Description	Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attac

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows Server 2003	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	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 Server 2003	-	All	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	All	All
Operating System	Microsoft	Windows Server 2003	-	sp1	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 Server 2008	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	All	All	All

Operating System	Microsoft	Windows Server 2008	-	All	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Vista	-	All	All	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Vista	-	sp1	All	All
Operating System	Microsoft	Windows Xp	-	All	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
Operating System	Microsoft	Windows Xp	-	All	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

References

Reference

US-CERT Technical Cyber Security Alert TA08-162B -- Microsoft Updates for Multiple Vulnerabilities

Microsoft Windows Pragmatic General Multicast Denial of Service - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Repository / Oval Repository

Webmail - OVH

SecurityTracker.com Archives - Windows Bug in Processing Pragmatic General Multicast Packets with an Invalid Fragment Option Lets Remo

Microsoft Security Bulletin MS08-036 - Important | Microsoft Docs

Microsoft Windows PGM Invalid Fragment Remote Denial Of Service Vulnerability

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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