



CVE-2006-2378

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

Summary

CVE	CVE-2006-2378
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-13 19:06:00 UTC
Updated	2021-07-23 12:55:00 UTC
Description	Buffer overflow in the ART Image Rendering component (jgdw400.dll) in Microsoft Windows XP SP1 and Sp2, Server 2003

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	le	5.0.1	All	All	All
Application	Microsoft	le	5.0.1	sp1	All	All
Application	Microsoft	le	5.0.1	sp2	All	All
Application	Microsoft	le	5.0.1	sp3	All	All
Application	Microsoft	le	5.0.1	sp4	All	All
Application	Microsoft	le	6.0	All	All	All
Application	Microsoft	le	6.0	sp1	All	All
Application	Microsoft	le	5.0.1	All	All	All
Application	Microsoft	le	5.0.1	sp1	All	All
Application	Microsoft	le	5.0.1	sp2	All	All
Application	Microsoft	le	5.0.1	sp3	All	All
Application	Microsoft	le	5.0.1	sp4	All	All
Application	Microsoft	le	6.0	All	All	All
Application	Microsoft	le	6.0	sp1	All	All
Application	Microsoft	Internet Explorer	5.0.1	All	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp1	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp2	All	All

Application	Microsoft	Internet Explorer	5.0.1	sp3	All	All
Application	Microsoft	Internet Explorer	5.0.1	sp4	All	All
Application	Microsoft	Internet Explorer	6.0	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	enterprise	All
Operating System	Microsoft	Windows 2003 Server	standard	All	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition_64-bit	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	r2	All	datacenter_64-bit	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	enterprise	All
Operating System	Microsoft	Windows 2003 Server	standard	All	All	All
Operating System	Microsoft	Windows 2003 Server	standard	sp1	All	All
Operating System	Microsoft	Windows 2003 Server	standard_64-bit	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	All	All	All
Operating System	Microsoft	Windows 2003 Server	web	sp1	All	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	home	All

Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All
Operating System	Microsoft	Windows Xp	All	All	64-bit	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	media_center	All
Operating System	Microsoft	Windows Xp	All	gold	professional	All
Operating System	Microsoft	Windows Xp	All	sp1	64-bit	All
Operating System	Microsoft	Windows Xp	All	sp1	home	All
Operating System	Microsoft	Windows Xp	All	sp1	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	home	All
Operating System	Microsoft	Windows Xp	All	sp2	media_center	All
Operating System	Microsoft	Windows Xp	All	sp2	tablet_pc	All

References

Reference

Microsoft Windows Malformed ART Image Remote Code Execution Vulnerability

IBM X-Force Exchange

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Repository / Oval Repository

26432

US-CERT Vulnerability Note VU#923236

Repository / Oval Repository

Repository / Oval Repository

Microsoft Security Bulletin MS06-022 - Critical | Microsoft Docs

Secunia - Advisories - Microsoft Windows ART Image Handling Buffer Overflow

Repository / Oval Repository

Repository / Oval Repository

Accenture | Let there be change

SecurityTracker.com Archives - Microsoft Windows Buffer Overflow in AOL ART Image Rendering Library Lets Remote Users Execute Arbitra

US-CERT Technical Cyber Security Alert TA06-164A -- Microsoft Windows, Internet Explorer, Media Player, Word, PowerPoint, and Exchange

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.

© [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 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](#)