



# CVE-2007-2227

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-2227
<b>State</b>	PUBLIC
<b>Assigner</b>	secure@microsoft.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-06-12 21:30:00 UTC
<b>Updated</b>	2018-10-16 16:42:00 UTC
<b>Description</b>	The MHTML protocol handler in Microsoft Outlook Express 6 and Windows Mail in Windows Vista does not properly handle

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Outlook Express	6.0	All	All	All
Application	Microsoft	Outlook Express	6.0	All	All	All
Operating System	Microsoft	Windows 2003 Server	All	All	x64	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	x64	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	All	All	x64	All
Operating System	Microsoft	Windows 2003 Server	All	sp2	x64	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	All	All
Operating System	Microsoft	Windows 2003 Server	sp1	All	itanium	All
Operating System	Microsoft	Windows 2003 Server	sp2	All	itanium	All
Application	Microsoft	Windows Mail	All	All	All	All
Application	Microsoft	Windows Mail	All	All	All	All
Operating System	Microsoft	Windows Vista	All	gold	All	All
Operating System	Microsoft	Windows Vista	All	gold	x64	All
Operating System	Microsoft	Windows Vista	All	gold	All	All

Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Vista</a>	All	gold	x64	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Xp</a>	All	All	professional_x64	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Xp</a>	All	sp2	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Xp</a>	All	sp2	professional_x64	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Xp</a>	All	All	professional_x64	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Xp</a>	All	sp2	All	All
Operating System	<a href="#">Microsoft</a>	<a href="#">Windows Xp</a>	All	sp2	professional_x64	All

## References

### Reference

401 Authorization Required

[Microsoft Security Bulletin MS07-034 - Critical | Microsoft Docs](#)

[SecurityTracker.com Archives - Outlook Express MHTML Protocol Handler Content-Disposition Bug Lets Remote Users Obtain Information](#)

[openmya.hacker.jp/hasegawa/security/ms07-034.txt](#)

[Repository / Oval Repository](#)

[Microsoft Outlook Express and Windows Mail Multiple Vulnerabilities - Advisories - Secunia](#)

35346

[SecurityTracker.com Archives - Windows Mail MHTML Protocol Handler Content-Disposition Bug Lets Remote Users Obtain Information](#)

[Microsoft Outlook Express Content Disposition Parsing Information Disclosure Vulnerability](#)

[SecurityFocus](#)

[SecurityFocus](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[US-CERT Technical Cyber Security Alert TA07-163A -- Microsoft Updates for Multiple Vulnerabilities](#)

[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](#).

