



# CVE-2008-3704

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

## Summary

<b>CVE</b>	CVE-2008-3704
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-08-18 19:41:00 UTC
<b>Updated</b>	2018-10-12 21:48:00 UTC
<b>Description</b>	Heap-based buffer overflow in the MaskedEdit ActiveX control in Msmask32.ocx 6.0.81.69, and possibly other versions bef

## Risk And Classification

**Problem Types: CWE-119**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Visual Basic	6.0	All	All	All
Application	Microsoft	Visual Basic	6.0	All	All	All
Application	Microsoft	Visual Foxpro	8.0	sp1	All	All
Application	Microsoft	Visual Foxpro	9.0	sp1	All	All
Application	Microsoft	Visual Foxpro	9.0	sp2	All	All
Application	Microsoft	Visual Foxpro	8.0	sp1	All	All
Application	Microsoft	Visual Foxpro	9.0	sp1	All	All
Application	Microsoft	Visual Foxpro	9.0	sp2	All	All
Application	Microsoft	Visual Studio	6.0	All	All	All
Application	Microsoft	Visual Studio	6.0	All	All	All
Application	Microsoft	Visual Studio .net	2002	sp1	All	All
Application	Microsoft	Visual Studio .net	2003	sp1	All	All
Application	Microsoft	Visual Studio .net	2002	sp1	All	All
Application	Microsoft	Visual Studio .net	2003	sp1	All	All

## References

Reference	Source
-----------	--------

Webmail - OVH	VUPEN
Visual Studio Buffer Overflow in 'Msmask32.ocx' ActiveX Control Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTR
Microsoft Security Bulletin MS08-070 - Critical   Microsoft Docs	MS
Repository / Oval Repository	OVAL
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Microsoft Visual Studio (Msmask32.ocx) ActiveX Remote BOF Exploit	EXPLOI
Microsoft Visual Studio 'Msmask32.ocx' ActiveX Control Remote Buffer Overflow Vulnerability	BID
ASA-2008-473 (ActiveX Controls) Could Allow Remote Code Execution (932349)	CONFIF
IBM X-Force Exchange	XF
Microsoft Visual Studio - 'Msmask32.ocx' ActiveX Remote Buffer Overflow (PoC) - Windows dos Exploit	EXPLOI
Microsoft Visual Studio Masked Edit Control "Mask" Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUN
US-CERT Technical Cyber Security Alert TA08-344A -- Microsoft Updates for Multiple Vulnerabilities	CERT
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)