



# CVE-2007-5197

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

## Summary

<b>CVE</b>	CVE-2007-5197
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-11-02 16:46:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	Buffer overflow in the Mono.Math.BigInteger class in Mono 1.2.5.1 and earlier allows context-dependent attackers to execute

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	powerpc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	s390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-32	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	powerpc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	s390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	4.0	All	sparc	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.0	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.0.5	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13.4	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13.6	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13.7	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.17	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.17.1	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.18	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.4	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.8.3	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.0	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.0.5	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13.4	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13.6	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.13.7	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.17	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.17.1	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.18	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.4	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	1.1.8.3	All	All	All
Application	<a href="#">Mono</a>	<a href="#">Mono</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	10.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	10.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	10.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	10.3	All	All	All
Operating System	<a href="#">Suse</a>	<a href="#">Suse Linux</a>	1.0	All	All	All

Operating System	Suse	Suse Linux	10	All	enterprise_desktop	All
Operating System	Suse	Suse Linux	10	All	enterprise_server	All
Operating System	Suse	Suse Linux	10	sp1	enterprise_desktop	All
Operating System	Suse	Suse Linux	10.0	All	personal	All
Operating System	Suse	Suse Linux	10.0	All	ppc	All
Operating System	Suse	Suse Linux	10.0	All	professional	All
Operating System	Suse	Suse Linux	10.0	All	x86	All
Operating System	Suse	Suse Linux	10.0	All	x86_64	All
Operating System	Suse	Suse Linux	10.1	All	personal	All
Operating System	Suse	Suse Linux	10.1	All	ppc	All
Operating System	Suse	Suse Linux	10.1	All	professional	All
Operating System	Suse	Suse Linux	10.1	All	x86	All
Operating System	Suse	Suse Linux	10.1	All	x86_64	All
Operating System	Suse	Suse Linux	10.2	All	personal	All
Operating System	Suse	Suse Linux	10.2	All	professional	All
Operating System	Suse	Suse Linux	8	All	enterprise_server	All
Operating System	Suse	Suse Linux	8.0	All	retail_solution	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	enterprise_server	All
Operating System	Suse	Suse Linux	1.0	All	All	All
Operating System	Suse	Suse Linux	10	All	enterprise_desktop	All
Operating System	Suse	Suse Linux	10	All	enterprise_server	All
Operating System	Suse	Suse Linux	10	sp1	enterprise_desktop	All
Operating System	Suse	Suse Linux	10.0	All	personal	All
Operating System	Suse	Suse Linux	10.0	All	ppc	All
Operating System	Suse	Suse Linux	10.0	All	professional	All
Operating System	Suse	Suse Linux	10.0	All	x86	All
Operating System	Suse	Suse Linux	10.0	All	x86_64	All
Operating System	Suse	Suse Linux	10.1	All	personal	All
Operating System	Suse	Suse Linux	10.1	All	ppc	All
Operating System	Suse	Suse Linux	10.1	All	professional	All
Operating System	Suse	Suse Linux	10.1	All	x86	All
Operating System	Suse	Suse Linux	10.1	All	x86_64	All
Operating System	Suse	Suse Linux	10.2	All	personal	All
Operating System	Suse	Suse Linux	10.2	All	professional	All

Operating System	Suse	Suse Linux	8	All	enterprise_server	All
Operating System	Suse	Suse Linux	8.0	All	retail_solution	All
Operating System	Suse	Suse Linux	9.0	All	All	All
Operating System	Suse	Suse Linux	9.0	All	enterprise_server	All
Application	Suse	Suse Linux Openexchange Server	4.0	All	All	All
Application	Suse	Suse Linux Openexchange Server	4.0	All	All	All
Operating System	Suse	Suse United Linux	1.0	All	All	All
Operating System	Suse	Suse United Linux	1.0	All	All	All

## References

Reference	Source	Link
Fedora update for mono - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Mandriva update for mono - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
USN-553-1: Mono vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
Ubuntu update for mono - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Debian -- Security Information -- DSA-1397-1 mono	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Debian update for mono - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
SUSE Update for Multiple Packages - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
367471 – (CVE-2007-5197) CVE-2007-5197: mono Math.BigInteger buffer overflow	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
Webmail- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Gentoo update for mono - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Mono Mono.Math.BigInteger Vulnerability - Advisories - Secunia	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Gentoo Linux Documentation -- Mono: Buffer overflow	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>
Gentoo Bug 197067 - dev-lang/mono < 1.2.5-r1 Buffer overflow in BigInteger (CVE-2007-5197)	CONFIRM	<a href="https://bugs.gentoo.org">bugs.gentoo.org</a>
Mono Integer Overflow May Let Local Users Gain Elevated Privileges - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
Support / Security / Advisories // MDKSA-2007:218   Mandriva	MANDRIVA	<a href="http://www.mandriva.com">www.mandriva.com</a>
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>
Mono System.Math BigInteger Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] Fedora 7 Update: mono-1.2.3-5.fc7	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
<a href="https://bugs.gentoo.org/attachment.cgi">bugs.gentoo.org/attachment.cgi</a>	CONFIRM	<a href="https://bugs.gentoo.org">bugs.gentoo.org</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

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](#)**