



CVE-2009-3658

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

Summary

CVE	CVE-2009-3658
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-10-09 14:30:00 UTC
Updated	2024-02-03 02:27:00 UTC
Description	Use-after-free vulnerability in the Sb.SuperBuddy.1 ActiveX control (sb.dll) in America Online (AOL) 9.5.0.1 allows remote a

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aol	Internet Software	9.1	All	All	All
Application	Aol	Internet Software	9.1	All	All	All
Application	Aol	Sb.superbuddy.1 Active X Control	9.5.0.1	All	All	All
Application	Aol	Sb.superbuddy.1 Active X Control	9.5.0.1	All	All	All
Application	Aol	Superbuddy Activex Control	9.5.0.1	All	All	All

References

Reference	Source
Webmail - OVH	VU
AOL SuperBuddy ActiveX Control Remote Code Execution Vulnerability	BI
Repository / Oval Repository	OV
AOL SuperBuddy ActiveX Control "SetSuperBuddy()" Memory Corruption - Secunia Advisories - Vulnerability Information - Secunia.com	SE
IBM X-Force Exchange	XF
Error 404 :(MI
SecurityFocus	BU
CVE Program record	CV
NVD vulnerability detail	NV

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](#)