



CVE-2007-5542

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

Summary

CVE	CVE-2007-5542
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-18 10:30:00 UTC
Updated	2009-03-18 10:30:00 UTC
Description	Stack-based buffer overflow in Miranda IM 0.6.8 allows remote attackers to execute arbitrary code via a crafted Yahoo! Mes

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Miranda-im	Miranda Im	0.6.8	All	All	All
Application	Miranda-im	Miranda Im	0.6.8	All	All	All

References

Reference

Files ≈ Packet Storm

Miranda Multiple Buffer Overflow Vulnerabilities

[Full-disclosure] Aircanner Mobile Security Advisory #07101401: Mobile-spy Victim/User Phone/SMS/URL Log Spoofing and Persistent XSS

Miranda IM Multiple Buffer Overflow Vulnerabilities - Research - SecureWorks: Managed, Monitored & On-Demand Security Services

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](#)