



CVE-2002-0377

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

Summary

CVE	CVE-2002-0377
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-05-29 04:00:00 UTC
Updated	2016-10-18 02:19:00 UTC
Description	Gaim 0.57 stores sensitive information in world-readable and group-writable files in the /tmp directory, which allows local us

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rob Flynn	Gaim	0.57	All	All	All
Application	Rob Flynn	Gaim	0.57	All	All	All

References

Reference
gaim.sourceforge.net/ChangeLog
Gaim Sensitive World Readable Temporary File Vulnerability
Neohapsis Archives - Vuln-Dev - Gaim arbitrary Email Reading - From smackenzsdf.lonestar.org
ISS X-Force Database: gaim-email-access (9061): Gaim chat client insecure /tmp files could allow an attacker to access a user's Hotmail acco
'Gaim arbitrary Email Reading' - MARC
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](#)