CVE-2002-0989

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2002-0989
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-09-24 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The URL handler in the manual browser option for Gaim before 0.59.1 allows remote attackers to execute arbitrary script vi

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rob Flynn	Gaim	0.51	All	All	All

Application	Rob Flynn	Gaim	0.52	All	All	All
Application	Rob Flynn	Gaim	0.53	All	All	All
Application	Rob Flynn	Gaim	0.54	All	All	All
Application	Rob Flynn	Gaim	0.55	All	All	All
Application	Rob Flynn	Gaim	0.56	All	All	All
Application	Rob Flynn	Gaim	0.57	All	All	All
Application	Rob Flynn	Gaim	0.58	All	All	All
Application	Rob Flynn	Gaim	0.59	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SN-02:06.asc
SecurityFocus HOME Advisories: Security vulnerability in gaim package
Home - Conectiva
Bug 72728 - gaim 0.59.1 is released with important security and bug fixes
gaim.sourceforge.net/ChangeLog
redhat.com | Red Hat Support
redhat.com | Red Hat Support
Debian -- Security Information -- DSA-158-1 gaim
frontal2.mandriva.com
Gaim Manual Browser Command Arbitrary Command Execution Vulnerability
www.osvdb.org/5033
redhat.com | Red Hat Support
ISS X-Force Database: gaim-url-handler-command-execution (9978): Gaim URL handler in "Manual" browser could allow command execution
redhat.com | Red Hat Support
'GLSA: gaim' - 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report