



# CVE-2005-3354

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

## Summary

<b>CVE</b>	CVE-2005-3354
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-11-20 21:03:00 UTC
<b>Updated</b>	2017-07-11 01:33:00 UTC
<b>Description</b>	Stack-based buffer overflow in the Idif_get_line function in Idif.c of Sylpheed before 2.1.6 allows user-assisted attackers to e

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.8.11	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.10	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.11	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.12	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.4	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.5	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.6	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.7	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.8	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	0.9.9	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	1.0.0	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	1.0.1	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	1.0.2	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	1.0.3	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	1.0.4	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	2.0	All	All	All
Application	<a href="#">Sylpheed</a>	<a href="#">Sylpheed</a>	2.0.1	All	All	All

Application	Sylpheed	Sylpheed	2.0.2	All	All	All
Application	Sylpheed	Sylpheed	2.0.3	All	All	All
Application	Sylpheed	Sylpheed	2.1	All	All	All
Application	Sylpheed	Sylpheed	2.1.1	All	All	All
Application	Sylpheed	Sylpheed	2.1.2	All	All	All
Application	Sylpheed	Sylpheed	2.1.3	All	All	All
Application	Sylpheed	Sylpheed	2.1.4	All	All	All
Application	Sylpheed	Sylpheed	2.1.5	All	All	All
Application	Sylpheed	Sylpheed	0.8.11	All	All	All
Application	Sylpheed	Sylpheed	0.9.10	All	All	All
Application	Sylpheed	Sylpheed	0.9.11	All	All	All
Application	Sylpheed	Sylpheed	0.9.12	All	All	All
Application	Sylpheed	Sylpheed	0.9.4	All	All	All
Application	Sylpheed	Sylpheed	0.9.5	All	All	All
Application	Sylpheed	Sylpheed	0.9.6	All	All	All
Application	Sylpheed	Sylpheed	0.9.7	All	All	All
Application	Sylpheed	Sylpheed	0.9.8	All	All	All
Application	Sylpheed	Sylpheed	0.9.9	All	All	All
Application	Sylpheed	Sylpheed	1.0.0	All	All	All
Application	Sylpheed	Sylpheed	1.0.1	All	All	All
Application	Sylpheed	Sylpheed	1.0.2	All	All	All
Application	Sylpheed	Sylpheed	1.0.3	All	All	All
Application	Sylpheed	Sylpheed	1.0.4	All	All	All
Application	Sylpheed	Sylpheed	2.0	All	All	All
Application	Sylpheed	Sylpheed	2.0.1	All	All	All
Application	Sylpheed	Sylpheed	2.0.2	All	All	All
Application	Sylpheed	Sylpheed	2.0.3	All	All	All
Application	Sylpheed	Sylpheed	2.1	All	All	All
Application	Sylpheed	Sylpheed	2.1.1	All	All	All
Application	Sylpheed	Sylpheed	2.1.2	All	All	All
Application	Sylpheed	Sylpheed	2.1.3	All	All	All
Application	Sylpheed	Sylpheed	2.1.4	All	All	All
Application	Sylpheed	Sylpheed	2.1.5	All	All	All

## References

Reference	Source	Link
Sylpheed LDIF Import Remote Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
Gentoo Linux Documentation -- Sylpheed, Sylpheed-Claws: Buffer overflow in LDIF importer	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>
Sylpheed - lightweight and user-friendly e-mail client	CONFIRM	<a href="http://sylpheed.good-day.net">sylpheed.good-day.net</a>
Secunia - Advisories - Debian update for sylpheed	SECUNIA	<a href="http://secunia.com">secunia.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Secunia - Advisories - SUSE Updates for Multiple Packages	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Secunia - Advisories - Sylpheed LDIF Import Buffer Overflow Vulnerability	SECUNIA	<a href="http://secunia.com">secunia.com</a>
20675	OSVDB	<a href="http://osvdb.org">osvdb.org</a>
Sylpheed buffer overflow FC3 - Xatrix Security	FEDORA	<a href="http://www.xatrix.org">www.xatrix.org</a>
Security Announcement	SUSE	<a href="http://www.novell.com">www.novell.com</a>
Debian -- Security Information -- DSA-906-1 sylpheed	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Gentoo update for sylpheed - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Fedora update for sylpheed - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</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](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/mitre).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)