



CVE-2005-0667

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2005-0667 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2005-03-07 05:00:00 UTC |
| Updated | 2008-09-05 20:46:00 UTC |
| Description | Buffer overflow in Sypheed before 1.0.3 and other versions before 1.9.5 allows remote attackers to execute arbitrary code |

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------|----------------------------------|---------|--------|------------------------|----------|
| Operating System | Altlinux | Alt Linux | 2.3 | All | compact | All |
| Operating System | Altlinux | Alt Linux | 2.3 | All | junior | All |
| Operating System | Altlinux | Alt Linux | 2.3 | All | compact | All |
| Operating System | Altlinux | Alt Linux | 2.3 | All | junior | All |
| Operating System | Gentoo | Linux | All | All | All | All |
| Operating System | Gentoo | Linux | All | All | All | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | advanced_server | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | advanced_server_ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | enterprise_server | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | enterprise_server_ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | workstation | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | workstation_ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | advanced_server | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | advanced_server_ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | enterprise_server | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | enterprise_server_ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | workstation | All |

| | | | | | | |
|------------------|----------|----------------------------|----------|-----|-------------------|-----|
| Operating System | Redhat | Enterprise Linux | 2.1 | All | workstation_ia64 | All |
| Operating System | Redhat | Fedora Core | core_3.0 | All | All | All |
| Operating System | Redhat | Fedora Core | core_3.0 | All | All | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | ia64 | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | itanium_processor | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | ia64 | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | itanium_processor | 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 | 0.9.99 | 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 | 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 | 0.9.99 | 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-claws | Sylpheed-claws | 1.0.2 | All | All | All |
| Application | Sylpheed-claws | Sylpheed-claws | 1.0.2 | All | All | All |

References

Reference

Sylpheed - a GTK+ based, lightweight, and fast e-mail client

rhn.redhat.com | Red Hat Support

Sylpheed - a GTK+ based, lightweight, and fast e-mail client

Gentoo Linux Documentation -- Sylpheed, Sylpheed-claws: Message reply overflow

Secunia - Advisories - Sylpheed Message Reply Buffer Overflow Vulnerability

SecurityTracker.com Archives - Sylpheed Buffer Overflow in Processing Message Headers May Let Remote Users Execute Arbitrary Code

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)