



CVE-2006-2198

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2006-2198 |
| State | PUBLIC |
| Assigner | security@debian.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2006-06-30 18:05:00 UTC |
| Updated | 2018-10-18 16:38:00 UTC |
| Description | OpenOffice.org (aka StarOffice) 1.1.x up to 1.1.5 and 2.0.x before 2.0.3 allows user-assisted attackers to conduct unauthori |

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------------------------|----------------------------|-----------|--------|---------|----------|
| Application | Openoffice | Openoffice | 1.1.0 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.1 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.1a | All | All | All |
| Application | Openoffice | Openoffice | 1.1.1b | All | All | All |
| Application | Openoffice | Openoffice | 1.1.2 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.3 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.4 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.5 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0_rc1 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0_rc2 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0_rc3 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.1 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc1 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc2 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc3 | All | All | All |

| | | | | | | |
|-------------|----------------------------|----------------------------|-----------|-----|-----|-----|
| Application | Openoffice | Openoffice | 2.0.2_rc4 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc3 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc4 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc5 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc6 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.0 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.1 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.1a | All | All | All |
| Application | Openoffice | Openoffice | 1.1.1b | All | All | All |
| Application | Openoffice | Openoffice | 1.1.2 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.3 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.4 | All | All | All |
| Application | Openoffice | Openoffice | 1.1.5 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0_rc1 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0_rc2 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.0_rc3 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.1 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc1 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc2 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc3 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.2_rc4 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc3 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc4 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc5 | All | All | All |
| Application | Openoffice | Openoffice | 2.0.3_rc6 | All | All | All |
| Application | Sun | Staroffice | 7.0 | All | All | All |
| Application | Sun | Staroffice | 8.0 | All | All | All |
| Application | Sun | Staroffice | 7.0 | All | All | All |
| Application | Sun | Staroffice | 8.0 | All | All | All |

References

Reference

Debian -- Security Information -- DSA-1104-2 [openoffice.org](#)

OpenOffice.org (OpenOffice) - Malware - Linux - All - CVE-2010-4003

StarOffice / StarSuite Multiple vulnerabilities - Advisories - Secunia

Ubuntu update for openoffice.org - Advisories - Secunia

Security Announcement

usn/usn-313-2 - Ubuntu: Linux for human beings

OpenOffice Arbitrary Macro Execution Vulnerability

rPath update for openoffice.org - Advisories - Secunia

[SECURITY] Fedora Core 5 Update: openoffice.org-2.0.2-5.20.2 | FedoraNEWS.ORG

usn/usn-313-1 - Ubuntu: Linux for human beings

Webmail - OVH

US-CERT Vulnerability Note VU#170113

Debian update for openoffice.org - Advisories - Secunia

Gentoo update for OpenOffice.org - Advisories - Secunia

Webmail - OVH

CVE-2006-2199

rhn.redhat.com | Red Hat Support

SecurityTracker.com Archives - OpenOffice.org Bugs Let Java Scripts Escape the Sandbox, Macro Code Be Executed, or Arbitrary Code Be E

SecurityFocus

Repository / Oval Repository

Fedora update for openoffice.org - Advisories - Secunia

#102490: Security Vulnerability With Macros in StarOffice/StarSuite

[#RPL-475] multiple openoffice.org vulnerabilities CVE-2006-2198 CVE-2006-3117 - rPath JIRA

Red Hat update for OpenOffice.org - Advisories - Secunia

OpenOffice Multiple Vulnerabilities - Advisories - Secunia

Mandriva update for OpenOffice.org - Advisories - Secunia

Gentoo Linux Documentation -- OpenOffice.org: Multiple vulnerabilities

IBM X-Force Exchange

SUSE update for OpenOffice_org - Advisories - Secunia

Advisories - Mandriva Linux

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](#)