



CVE-2006-1173

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-1173
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-07 23:06:00 UTC
Updated	2018-10-18 16:31:00 UTC
Description	Sendmail before 8.13.7 allows remote attackers to cause a denial of service via deeply nested, malformed multipart MIME r

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sendmail	Sendmail	8.10	All	All	All
Application	Sendmail	Sendmail	8.10.1	All	All	All
Application	Sendmail	Sendmail	8.10.2	All	All	All
Application	Sendmail	Sendmail	8.11.0	All	All	All
Application	Sendmail	Sendmail	8.11.1	All	All	All
Application	Sendmail	Sendmail	8.11.2	All	All	All
Application	Sendmail	Sendmail	8.11.3	All	All	All
Application	Sendmail	Sendmail	8.11.4	All	All	All
Application	Sendmail	Sendmail	8.11.5	All	All	All
Application	Sendmail	Sendmail	8.11.6	All	All	All
Application	Sendmail	Sendmail	8.11.7	All	All	All
Application	Sendmail	Sendmail	8.12	beta10	All	All
Application	Sendmail	Sendmail	8.12	beta12	All	All
Application	Sendmail	Sendmail	8.12	beta16	All	All
Application	Sendmail	Sendmail	8.12	beta5	All	All
Application	Sendmail	Sendmail	8.12	beta7	All	All
Application	Sendmail	Sendmail	8.12.0	All	All	All

Application	Sendmail	Sendmail	8.12.1	All	All	All
Application	Sendmail	Sendmail	8.12.10	All	All	All
Application	Sendmail	Sendmail	8.12.11	All	All	All
Application	Sendmail	Sendmail	8.12.2	All	All	All
Application	Sendmail	Sendmail	8.12.3	All	All	All
Application	Sendmail	Sendmail	8.12.4	All	All	All
Application	Sendmail	Sendmail	8.12.5	All	All	All
Application	Sendmail	Sendmail	8.12.6	All	All	All
Application	Sendmail	Sendmail	8.12.7	All	All	All
Application	Sendmail	Sendmail	8.12.8	All	All	All
Application	Sendmail	Sendmail	8.12.9	All	All	All
Application	Sendmail	Sendmail	8.13.0	All	All	All
Application	Sendmail	Sendmail	8.13.1	All	All	All
Application	Sendmail	Sendmail	8.13.1.2	All	All	All
Application	Sendmail	Sendmail	8.13.2	All	All	All
Application	Sendmail	Sendmail	8.13.3	All	All	All
Application	Sendmail	Sendmail	8.13.4	All	All	All
Application	Sendmail	Sendmail	8.13.5	All	All	All
Application	Sendmail	Sendmail	8.8.8	All	All	All
Application	Sendmail	Sendmail	8.9.0	All	All	All
Application	Sendmail	Sendmail	8.9.1	All	All	All
Application	Sendmail	Sendmail	8.9.2	All	All	All
Application	Sendmail	Sendmail	8.9.3	All	All	All
Application	Sendmail	Sendmail	8.10	All	All	All
Application	Sendmail	Sendmail	8.10.1	All	All	All
Application	Sendmail	Sendmail	8.10.2	All	All	All
Application	Sendmail	Sendmail	8.11.0	All	All	All
Application	Sendmail	Sendmail	8.11.1	All	All	All
Application	Sendmail	Sendmail	8.11.2	All	All	All
Application	Sendmail	Sendmail	8.11.3	All	All	All
Application	Sendmail	Sendmail	8.11.4	All	All	All
Application	Sendmail	Sendmail	8.11.5	All	All	All
Application	Sendmail	Sendmail	8.11.6	All	All	All
Application	Sendmail	Sendmail	8.11.7	All	All	All
Application	Sendmail	Sendmail	8.12	beta10	All	All

Application	Sendmail	Sendmail	8.12	beta12	All	All
Application	Sendmail	Sendmail	8.12	beta16	All	All
Application	Sendmail	Sendmail	8.12	beta5	All	All
Application	Sendmail	Sendmail	8.12	beta7	All	All
Application	Sendmail	Sendmail	8.12.0	All	All	All
Application	Sendmail	Sendmail	8.12.1	All	All	All
Application	Sendmail	Sendmail	8.12.10	All	All	All
Application	Sendmail	Sendmail	8.12.11	All	All	All
Application	Sendmail	Sendmail	8.12.2	All	All	All
Application	Sendmail	Sendmail	8.12.3	All	All	All
Application	Sendmail	Sendmail	8.12.4	All	All	All
Application	Sendmail	Sendmail	8.12.5	All	All	All
Application	Sendmail	Sendmail	8.12.6	All	All	All
Application	Sendmail	Sendmail	8.12.7	All	All	All
Application	Sendmail	Sendmail	8.12.8	All	All	All
Application	Sendmail	Sendmail	8.12.9	All	All	All
Application	Sendmail	Sendmail	8.13.0	All	All	All
Application	Sendmail	Sendmail	8.13.1	All	All	All
Application	Sendmail	Sendmail	8.13.1.2	All	All	All
Application	Sendmail	Sendmail	8.13.2	All	All	All
Application	Sendmail	Sendmail	8.13.3	All	All	All
Application	Sendmail	Sendmail	8.13.4	All	All	All
Application	Sendmail	Sendmail	8.13.5	All	All	All
Application	Sendmail	Sendmail	8.8.8	All	All	All
Application	Sendmail	Sendmail	8.9.0	All	All	All
Application	Sendmail	Sendmail	8.9.1	All	All	All
Application	Sendmail	Sendmail	8.9.2	All	All	All
Application	Sendmail	Sendmail	8.9.3	All	All	All
Application	Sendmail	Sendmail	All	All	All	All

References

Reference

#102460: A Security Vulnerability in sendmail(1M) Versions Prior to 8.13.7 May Allow a Denial of Service (DoS) To Occur

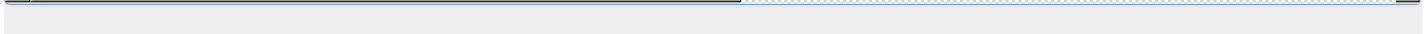
Sendmail Malformed MIME Message Denial Of Service Vulnerability

26197

Mandriva update for sendmail - Advisories - Secunia

Webmail - OVH
IBM X-Force Exchange
HP Tru64 UNIX and HP Internet Express Sendmail Vulnerability - Advisories - Secunia
Debian update for sendmail - Advisories - Secunia
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: sendmail remote denial of service attack (SUSE-SA
IT Resource Center - login / register
Avaya CMS / IR Sun Solaris Sendmail Denial of Service - Advisories - Secunia
Webmail - OVH
Webmail - OVH
SecurityFocus
Webmail - OVH
FreeBSD-SA-06:17.sendmail
SecurityFocus
Slackware update for sendmail - Advisories - Secunia
Gentoo Linux Documentation -- Sendmail: Denial of Service
OpenBSD update for sendmail - Advisories - Secunia
SecurityTracker.com Archives - Sendmail Excessive Recursion in Processing Malformed MIME Messages Lets Remote Users Deny Service
20060601-01-P
OpenBSD 3.8 errata
SecurityFocus
Search results
Advisories - Mandriva Linux
SGI IRIX update for sendmail - Advisories - Secunia
Webmail - OVH
Red Hat update for sendmail - Advisories - Secunia
ASA-2006-148 (SUN 102460, 102461)
rPath update for sendmail - Advisories - Secunia
Repository / Oval Repository
F-Secure Messaging Security Gateway Sendmail Vulnerability - Advisories - Secunia
[#RPL-526] sendmail DoS attack CVE-2006-1173 - rPath JIRA
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
20060602-01-U
Gentoo update for sendmail - Advisories - Secunia
SecurityFocus
Webmail - OVH

Solaris update for sendmail - Advisories - Secunia
HP-UX update for Sendmail - Advisories - Secunia
IBM Search results - United States
FortiGuard Center - FortiGuard Advisory - Advisory – SMTP Sendmail Email Vulnerability (VU# 146718)
Webmail - OVH
Sendmail Multi-Part MIME Message Handling Denial of Service - Advisories - Secunia
SUSE update for sendmail - Advisories - Secunia
SecurityFocus
F-Secure Security Bulletin FSC-2006-5
US-CERT Vulnerability Note VU#146718
Sendmail Sentrion Open Source - Open Source Email Server Proofpoint
Debian -- Security Information -- DSA-1155-2 sendmail
FortiMail Sendmail Multi-Part MIME Message Handling Vulnerability - Advisories - Secunia
FreeBSD update for sendmail - Advisories - Secunia
rhn.redhat.com Red Hat Support
IBM AIX update for Sendmail - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories
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](#)