



CVE-2006-0058

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

Summary

CVE	CVE-2006-0058
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-03-22 20:06:00 UTC
Updated	2018-10-19 15:42:00 UTC
Description	Signal handler race condition in Sendmail 8.13.x before 8.13.6 allows remote attackers to execute arbitrary code by triggeri

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sendmail	Sendmail	8.13.0	All	All	All
Application	Sendmail	Sendmail	8.13.1	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	8.13.0	All	All	All
Application	Sendmail	Sendmail	8.13.1	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

References

Reference
FreeBSD-SA-06:13
24037

Q-151: sendmail Security Update
HPSBUX02108
Sendmail Signal Handling Memory Corruption Vulnerability - Advisories - Secunia
NetBSD Sendmail Memory Corruption Vulnerability - Advisories - Secunia
Security Announcement
IT Resource Center - login / register
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Sendmail.com - Enterprise solutions for secure, dependable and compliant messaging
Avaya Products Sendmail Signal Handling Memory Corruption - Advisories - Secunia
Repository / Oval Repository
#102324: Sun Cobalt sendmail(8) Security Issue Involving Signal Handling Daemon
Webmail - OVH
SecurityTracker.com Archives - Sendmail Race Condition in Signal Handler May Let Remote Users Trigger a Buffer Overflow to Execute Arbit
Webmail - OVH
Sendmail Asynchronous Signal Handling Remote Code Execution Vulnerability
SCOSA-2006.24
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
216
Gentoo Linux Documentation -- Sendmail: Race condition in the handling of asynchronous signals
Gentoo update for sendmail - Advisories - Secunia
Support Red Hat
OpenBSD 3.8 errata
support.avaya.com/elmodocs2/security/ASA-2006-078.htm
Debian update for sendmail - Advisories - Secunia
AIX sendmail Signal Handling Memory Corruption Vulnerability - Advisories - Secunia
IBM X-Force Exchange
Repository / Oval Repository
F-Secure Messaging Security Gateway Sendmail Vulnerability - Advisories - Secunia
Search results
SecurityFocus
UnixWare update for Sendmail - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories
20060302-01-P
US-CERT Vulnerability Note VU#834865
Red Hat update for sendmail - Advisories - Secunia
Q-151: sendmail Security Update

Slackware update for sendmail - Advisories - Secunia
OpenBSD update for sendmail - Advisories - Secunia
20060401-01-U
Advisories - Mandriva Linux
IBM Support: Fix Central
Search results
US-CERT Technical Cyber Security Alert TA06-081A -- Sendmail Race Condition Vulnerability
SecurityReason
Sun Cobalt Sendmail Memory Corruption Vulnerability - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Sun Solaris Sendmail Signal Handling Memory Corruption - Advisories - Secunia
SGI IRIX update for sendmail - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
[SECURITY] Fedora Core 4 Update: sendmail-8.13.6-0.FC4.1
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
About Secunia Research Flexera
Avaya CMS / IR Sendmail Memory Corruption Vulnerability - Advisories - Secunia
Fedora update for sendmail - Advisories - Secunia
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia
SecurityFocus
#102262: Security Vulnerability in sendmail(1M) Versions Prior to 8.13.6
F-Secure Security Bulletin FSC-2006-2
SUSE update for sendmail - Advisories - Secunia
SecurityReason - HP-UX running Sendmail, Remote Execution of Arbitrary Code
www14.software.ibm.com/webapp/set2/subscriptions/pqvcmj
FreeBSD update for sendmail - Advisories - Secunia
1. Overview:
OpenPKG Corporation: Security: Security Advisories
Search results
NetBSD-SA2006-010
HP-UX update for sendmail - Advisories - Secunia
Support Red Hat
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
200494
Debian -- Security Information -- DSA-1015-1 sendmail

[SECURITY] Fedora Core 5 Update: sendmail-8.13.6-0.FC5.1

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](#)