



CVE-2002-2261

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

Summary

CVE	CVE-2002-2261
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-12-31 05:00:00 UTC
Updated	2017-10-11 01:29:00 UTC
Description	Sendmail 8.9.0 through 8.12.6 allows remote attackers to bypass relaying restrictions enforced by the 'check_relay' function

Risk And Classification

Problem Types: CWE-264

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	8.10.0	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	8.12.2	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	8.9.0	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	8.10.0	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	8.12.2	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	8.9.0	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

References

Reference	Source	Link
Repository / Oval Repository	OVAL	oval.cisecurity.org/
20030101-01-P	SGI	patches.sgi.com/
Repository / Oval Repository	OVAL	oval.cisecurity.org/
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com/
Sendmail - 8.12	CONFIRM	www.sendmail.com/
Sendmail 'check_relay' E-mail Access Control Features Can Be Bypassed By Remote Users - SecurityTracker	SECTRACK	securitytracker.com/
Sendmail check_relay Access Bypassing Vulnerability	BID	www.securityfocus.com/bid/
Secunia - Advisories - IRIX updates to sendmail	SECUNIA	secunia.com/
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/
CVE Program record	CVE.ORG	www.cve.org/
NVD vulnerability detail	NVD	nvd.nist.gov/

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