



CVE-2017-16944

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

Summary

CVE	CVE-2017-16944
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-25 17:29:00 UTC
Updated	2021-05-04 18:15:00 UTC
Description	The receive_msg function in receive.c in the SMTP daemon in Exim 4.88 and 4.89 allows remote attackers to cause a denial of service (CPU consumption) by sending a large number of messages.

Risk And Classification

Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Exim	Exim	4.88	All	All	All
Application	Exim	Exim	4.89	All	All	All
Application	Exim	Exim	4.88	All	All	All
Application	Exim	Exim	4.89	All	All	All

References

Reference	Source	Link
oss-security - 21Nails: Multiple vulnerabilities in Exim	MLIST	www.openwall.com
Debian -- Security Information -- DSA-4053-1 exim4	DEBIAN	www.debian.org
Exim Infinite Loop in bdat_getc() Lets Remote Users Consume Excessive Memory Resources - SecurityTracker	SECTRACK	www.securitytracker.com
Bug 2201 – Exim handles BDAT data incorrectly and leads to crash	MISC	bugs.exim.org
oss-security - Re: RCE in Exim reported	MISC	openwall.com
Exim 4.89 - 'BDAT' Denial of Service - Multiple dos Exploit	EXPLOIT-DB	www.exploit-db.com
oss-security - RCE in Exim reported	MISC	openwall.com
oss-security - Re: RCE in Exim reported	MISC	openwall.com

[exim-announce] Critical Exim Security Vulnerability: disable chunking	MISC	lists.exim.o
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.go

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [500886](#) Alpine Linux Security Update for exim
- [504719](#) Alpine Linux Security Update for exim
- [710286](#) Gentoo Linux Exim Multiple Vulnerabilities (GLSA 201803-01)
- [750227](#) OpenSUSE Security Update for exim (openSUSE-SU-2021:0677-1)

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report