



CVE-2007-4321

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

Summary

CVE	CVE-2007-4321
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-14 00:17:00 UTC
Updated	2012-10-31 02:41:00 UTC
Description	fail2ban 0.8 and earlier does not properly parse sshd log files, which allows remote attackers to add arbitrary hosts to the /e

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fail2ban	Fail2ban	0.8	All	All	All
Application	Fail2ban	Fail2ban	0.8	All	All	All

References

Reference	Source	Link	Tags
Gentoo Bug 181214 - net-analyzer/fail2ban < 0.8.0-r1 Log injection (CVE-2007-4321)	MISC	bugs.gentoo.org	
OSSEC HIDS - Open Source Security	MISC	www.ossec.net	
Debian update for fail2ban - Secunia.com	SECUNIA	secunia.com	
Fail2ban Remote Denial of Service Vulnerability	BID	www.securityfocus.com	
Fail2ban: Denial of Service — Gentoo Linux Documentation	GENTOO	security.gentoo.org	
42484	OSVDB	osvdb.org	
Fail2ban Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	secunia.com	
Debian -- Security Information -- DSA-1456-1 fail2ban	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)