



CVE-2021-32749

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

Summary

CVE	CVE-2021-32749
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-16 18:15:00 UTC
Updated	2023-11-07 03:35:00 UTC
Description	fail2ban is a daemon to ban hosts that cause multiple authentication errors. In versions 0.9.7 and prior, 0.10.0 through 0.10

Risk And Classification

Problem Types: CWE-94

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fail2ban	Fail2ban	All	All	All	All
Application	Fail2ban	Fail2ban	All	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All

References

Reference	Source	Link
GNU Mailutils: unexpected processsing of escape sequences (GLSA 202310-13) — Gentoo security	GENTOO	security.gentoo.c
[SECURITY] Fedora 35 Update: fail2ban-0.11.2-9.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
[SECURITY] Fedora 35 Update: fail2ban-0.11.2-9.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraprojec
[SECURITY] Fedora 34 Update: fail2ban-0.11.2-9.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraprojec
fixed possible RCE vulnerability, unset escape variable (default tild... · fail2ban/fail2ban@410a6ce · GitHub	MISC	github.com
[SECURITY] Fedora 34 Update: fail2ban-0.11.2-9.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraprojec
Possible RCE vulnerability in mailing action using mailutils (mail-whois) · Advisory · fail2ban/fail2ban · GitHub	CONFIRM	github.com
fixed possible RCE vulnerability, unset escape variable (default tild... · fail2ban/fail2ban@2ed414e · GitHub	MISC	github.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.

Legacy QID Mappings

[179503](#) Debian Security Update for fail2ban (CVE-2021-32749)

[281997](#) Fedora Security Update for fail2ban (FEDORA-2021-0ab8f6a19a)

[501956](#) Alpine Linux Security Update for fail2ban

[502215](#) Alpine Linux Security Update for fail2ban

[503920](#) Alpine Linux Security Update for fail2ban

[690199](#) Free Berkeley Software Distribution (FreeBSD) Security Update for fail2ban (c848059a-318b-11ec-aa15-0800270512f4)

[710773](#) Gentoo Linux GNU Mailutils unexpected processing of escape sequences Vulnerability (GLSA 202310-13)

[751147](#) OpenSUSE Security Update for fail2ban (openSUSE-SU-2021:1274-1)

© [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](#)