



# CVE-2021-33582

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

## Summary

<b>CVE</b>	CVE-2021-33582
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-09-01 06:15:00 UTC
<b>Updated</b>	2023-11-07 03:35:00 UTC
<b>Description</b>	Cyrus IMAP before 3.4.2 allows remote attackers to cause a denial of service (multiple-minute daemon hang) via input that

## Risk And Classification

**Problem Types:** CWE-407

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cyrus</a>	<a href="#">Imap</a>	All	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 34 Update: cyrus-imapd-3.2.8-2.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Release Notes — Cyrus IMAP 3.4.1 documentation	MISC	<a href="https://www.cyrusimap.org">www.cyrusimap.org</a>
[SECURITY] [DLA 3052-1] cyrus-imapd security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>
Security Advisories · cyrusimap/cyrus-imapd · GitHub	MISC	<a href="https://github.com">github.com</a>
Topicbox	CONFIRM	<a href="https://cyrus.topicbox.com">cyrus.topicbox.com</a>
[SECURITY] Fedora 35 Update: cyrus-imapd-3.2.8-2.fc35 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 34 Update: cyrus-imapd-3.2.8-2.fc34 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
[SECURITY] Fedora 35 Update: cyrus-imapd-3.2.8-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Commits · cyrusimap/cyrus-imapd · GitHub	MISC	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

159384	Oracle Enterprise Linux Security Update for cyrus-imapd (ELSA-2021-3492)
179376	Debian Security Update for cyrus-imapd (DLA 3052-1)
179841	Debian Security Update for cyrus-imapd (CVE-2021-33582)
239632	Red Hat Update for cyrus-imapd (RHSA-2021:3493)
239633	Red Hat Update for cyrus-imapd (RHSA-2021:3492)
239643	Red Hat Update for cyrus-imapd (RHSA-2021:3546)
282409	Fedora Security Update for cyrus (FEDORA-2022-c30b1a8aa3)
282414	Fedora Security Update for cyrus (FEDORA-2022-d45bcc5447)
353081	Amazon Linux Security Advisory for cyrus-imapd : ALAS2-2021-1725
353115	Amazon Linux Security Advisory for cyrus-imapd : ALAS-2022-1559
377093	Alibaba Cloud Linux Security Update for cyrus-imapd (ALINUX3-SA-2021:0067)
690048	Free Berkeley Software Distribution (FreeBSD) Security Update for cyrus-imapd (3d915d96-0b1f-11ec-8d9f-080027415d17)
940350	AlmaLinux Security Update for cyrus-imapd (ALSA-2021:3492)
960013	Rocky Linux Security Update for cyrus-imapd (RLSA-2021:3492)

© [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](#)