



# CVE-2015-8077

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

## Summary

<b>CVE</b>	CVE-2015-8077
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-12-03 20:59:00 UTC
<b>Updated</b>	2023-11-07 02:28:00 UTC
<b>Description</b>	Integer overflow in the index_urfetech function in imap/index.c in Cyrus IMAP 2.3.19, 2.4.18, and 2.5.6 allows remote attack

## Risk And Classification

**Problem Types: CWE-189**

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cyrus	Imap	2.3.0	All	All	All
Application	Cyrus	Imap	2.3.1	All	All	All
Application	Cyrus	Imap	2.3.10	All	All	All
Application	Cyrus	Imap	2.3.11	All	All	All
Application	Cyrus	Imap	2.3.12	All	All	All
Application	Cyrus	Imap	2.3.13	All	All	All
Application	Cyrus	Imap	2.3.14	All	All	All
Application	Cyrus	Imap	2.3.15	All	All	All
Application	Cyrus	Imap	2.3.16	All	All	All
Application	Cyrus	Imap	2.3.17	All	All	All
Application	Cyrus	Imap	2.3.18	All	All	All
Application	Cyrus	Imap	2.3.2	All	All	All
Application	Cyrus	Imap	2.3.3	All	All	All
Application	Cyrus	Imap	2.3.4	All	All	All
Application	Cyrus	Imap	2.3.5	All	All	All
Application	Cyrus	Imap	2.3.6	All	All	All
Application	Cyrus	Imap	2.3.7	All	All	All

Application	Cyrus	Imap	2.3.8	All	All	All
Application	Cyrus	Imap	2.3.9	All	All	All
Application	Cyrus	Imap	2.4.0	All	All	All
Application	Cyrus	Imap	2.4.1	All	All	All
Application	Cyrus	Imap	2.4.10	All	All	All
Application	Cyrus	Imap	2.4.11	All	All	All
Application	Cyrus	Imap	2.4.12	All	All	All
Application	Cyrus	Imap	2.4.13	All	All	All
Application	Cyrus	Imap	2.4.14	All	All	All
Application	Cyrus	Imap	2.4.15	All	All	All
Application	Cyrus	Imap	2.4.16	All	All	All
Application	Cyrus	Imap	2.4.17	All	All	All
Application	Cyrus	Imap	2.4.2	All	All	All
Application	Cyrus	Imap	2.4.3	All	All	All
Application	Cyrus	Imap	2.4.4	All	All	All
Application	Cyrus	Imap	2.4.5	All	All	All
Application	Cyrus	Imap	2.4.6	All	All	All
Application	Cyrus	Imap	2.4.7	All	All	All
Application	Cyrus	Imap	2.4.8	All	All	All
Application	Cyrus	Imap	2.4.9	All	All	All
Application	Cyrus	Imap	2.5.0	All	All	All
Application	Cyrus	Imap	2.5.1	All	All	All
Application	Cyrus	Imap	2.5.2	All	All	All
Application	Cyrus	Imap	2.5.3	All	All	All
Application	Cyrus	Imap	2.3.0	All	All	All
Application	Cyrus	Imap	2.3.1	All	All	All
Application	Cyrus	Imap	2.3.10	All	All	All
Application	Cyrus	Imap	2.3.11	All	All	All
Application	Cyrus	Imap	2.3.12	All	All	All
Application	Cyrus	Imap	2.3.13	All	All	All
Application	Cyrus	Imap	2.3.14	All	All	All
Application	Cyrus	Imap	2.3.15	All	All	All
Application	Cyrus	Imap	2.3.16	All	All	All
Application	Cyrus	Imap	2.3.17	All	All	All
Application	Cyrus	Imap	2.3.18	All	All	All

Application	Cyrus	Imap	2.3.2	All	All	All
Application	Cyrus	Imap	2.3.3	All	All	All
Application	Cyrus	Imap	2.3.4	All	All	All
Application	Cyrus	Imap	2.3.5	All	All	All
Application	Cyrus	Imap	2.3.6	All	All	All
Application	Cyrus	Imap	2.3.7	All	All	All
Application	Cyrus	Imap	2.3.8	All	All	All
Application	Cyrus	Imap	2.3.9	All	All	All
Application	Cyrus	Imap	2.4.0	All	All	All
Application	Cyrus	Imap	2.4.1	All	All	All
Application	Cyrus	Imap	2.4.10	All	All	All
Application	Cyrus	Imap	2.4.11	All	All	All
Application	Cyrus	Imap	2.4.12	All	All	All
Application	Cyrus	Imap	2.4.13	All	All	All
Application	Cyrus	Imap	2.4.14	All	All	All
Application	Cyrus	Imap	2.4.15	All	All	All
Application	Cyrus	Imap	2.4.16	All	All	All
Application	Cyrus	Imap	2.4.17	All	All	All
Application	Cyrus	Imap	2.4.2	All	All	All
Application	Cyrus	Imap	2.4.3	All	All	All
Application	Cyrus	Imap	2.4.4	All	All	All
Application	Cyrus	Imap	2.4.5	All	All	All
Application	Cyrus	Imap	2.4.6	All	All	All
Application	Cyrus	Imap	2.4.7	All	All	All
Application	Cyrus	Imap	2.4.8	All	All	All
Application	Cyrus	Imap	2.4.9	All	All	All
Application	Cyrus	Imap	2.5.0	All	All	All
Application	Cyrus	Imap	2.5.1	All	All	All
Application	Cyrus	Imap	2.5.2	All	All	All
Application	Cyrus	Imap	2.5.3	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

Reference	Source	Link	Tags
Cyrus IMAP Server Integer Overflows Have Unspecified Impact - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>	
openSUSE-SU-2015:2200-1: moderate: Security update for cyrus-imapd	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
oss-security - Re: CVE request: urlfetch range handling flaw in Cyrus IMAP	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
Recent security fixes	MLIST	<a href="http://lists.andrew.cmu.edu">lists.andrew.cmu.edu</a>	
cyrus.foundation/cyrus-imapd/commit	CONFIRM	<a href="http://cyrus.foundation">cyrus.foundation</a>	
[security-announce] SUSE-SU-2016:1457-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
[security-announce] SUSE-SU-2016:1459-1: important: Security update for	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
Cyrus IMAP 2.5.7 Release Notes — Cyrus IMAP and SASL documentation	CONFIRM	<a href="http://docs.cyrus.foundation">docs.cyrus.foundation</a>	Vendor Adviso
openSUSE-SU-2015:2130-1: moderate: cyrus-imapd	SUSE	<a href="http://lists.opensuse.org">lists.opensuse.org</a>	
oss-security - Re: CVE request: urlfetch range handling flaw in Cyrus IMAP	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, anal

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)