



CVE-2014-0664

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

Summary

CVE	CVE-2014-0664
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-10 16:47:00 UTC
Updated	2017-08-29 01:34:00 UTC
Description	The server in Cisco Unity Connection allows remote authenticated users to cause a denial of service (CPU consumption) vi

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unity Connection	-	All	All	All
Application	Cisco	Unity Connection	-	All	All	All

References

Reference	Source
Security Advisory SA56370 - Cisco Unity Connection IMAP UID SEARCH Command Denial of Service Vulnerability - Secunia	SECUNIA
101915	OSVDB
Cisco Unity Connection IMAP Function Denial of Service Vulnerability	BID
Cisco Unity Connection IMAP Processing Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	SECTrack
Cisco Security Notice: Cisco Unity Connection Internet Message Access Protocol Denial of Service Vulnerability	CISCO
IBM X-Force Exchange	XF
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#)