



CVE-2008-3814

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

Summary

CVE	CVE-2008-3814
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-08 22:00:00 UTC
Updated	2017-08-08 01:32:00 UTC
Description	Unspecified vulnerability in Cisco Unity 4.x before 4.2(1)ES161, 5.x before 5.0(1)ES53, and 7.x before 7.0(2)ES8, when usi

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unity	4.0	All	All	All
Application	Cisco	Unity	4.0(1)	All	All	All
Application	Cisco	Unity	4.0(2)	All	All	All
Application	Cisco	Unity	4.0(3)	All	All	All
Application	Cisco	Unity	4.0(3)	sr1	All	All
Application	Cisco	Unity	4.0(4)	All	All	All
Application	Cisco	Unity	4.0(4)	sr1	All	All
Application	Cisco	Unity	4.0(5)	All	All	All
Application	Cisco	Unity	4.0\1\	All	All	All
Application	Cisco	Unity	4.0\2\	All	All	All
Application	Cisco	Unity	4.0\3\	All	All	All
Application	Cisco	Unity	4.0\3\	sr1	All	All
Application	Cisco	Unity	4.0\4\	All	All	All
Application	Cisco	Unity	4.0\4\	sr1	All	All
Application	Cisco	Unity	4.0\5\	All	All	All
Application	Cisco	Unity	4.1(1)	All	All	All
Application	Cisco	Unity	4.1\1\	All	All	All

Application	Cisco	Unity	4.2(1)	All	All	All
Application	Cisco	Unity	4.2\\(1\\)	All	All	All
Application	Cisco	Unity	5.0	All	All	All
Application	Cisco	Unity	5.0(1)	All	All	All
Application	Cisco	Unity	5.0\\(1\\)	All	All	All
Application	Cisco	Unity	7.0	All	All	All
Application	Cisco	Unity	7.0(2)	All	All	All
Application	Cisco	Unity	7.0\\(2\\)	All	All	All
Application	Cisco	Unity	4.0	All	All	All
Application	Cisco	Unity	4.0\\(1\\)	All	All	All
Application	Cisco	Unity	4.0\\(2\\)	All	All	All
Application	Cisco	Unity	4.0\\(3\\)	All	All	All
Application	Cisco	Unity	4.0\\(3\\)	sr1	All	All
Application	Cisco	Unity	4.0\\(4\\)	All	All	All
Application	Cisco	Unity	4.0\\(4\\)	sr1	All	All
Application	Cisco	Unity	4.0\\(5\\)	All	All	All
Application	Cisco	Unity	4.1\\(1\\)	All	All	All
Application	Cisco	Unity	4.2\\(1\\)	All	All	All
Application	Cisco	Unity	5.0	All	All	All
Application	Cisco	Unity	5.0\\(1\\)	All	All	All
Application	Cisco	Unity	7.0	All	All	All
Application	Cisco	Unity	7.0\\(2\\)	All	All	All

References						
Reference						Source
Cisco Unity 7.0 Multiple Remote Vulnerabilities						BID
Cisco Security Response: VoIPshield Reported Vulnerabilities in Cisco Unity Server [Products & Services] - Cisco Systems						CISCO
Cisco Security Advisory: Authentication Bypass in Cisco Unity [Products & Services] - Cisco Systems						CISCO
Cisco Unity Remote Administration Authentication Bypass Vulnerability						BID
Cisco Unity Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com						SECUNIA
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUPEN
IBM X-Force Exchange						XF
Nothing found for Research Details Php?id=126						MISC
Cisco Unity Authentication Bypass Bug Lets Remote Users View and Modify the Configuration - SecurityTracker						SECTRACK
CVE Program record						CVE.ORG
CVE Program record						CVE

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](#)