



CVE-2009-2047

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2009-2047
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-16 15:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Directory traversal vulnerability in the Administration interface in Cisco Customer Response Solutions (CRS) before 7.0(1) S

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Crs	3.5	All	All	All
Application	Cisco	Crs	4.0	All	All	All
Application	Cisco	Crs	4.1	All	All	All
Application	Cisco	Crs	4.5	All	All	All
Application	Cisco	Crs	5.0	All	All	All
Application	Cisco	Crs	6.0	All	All	All
Application	Cisco	Crs	7.0	All	All	All
Application	Cisco	Crs	3.5	All	All	All
Application	Cisco	Crs	4.0	All	All	All
Application	Cisco	Crs	4.1	All	All	All
Application	Cisco	Crs	4.5	All	All	All
Application	Cisco	Crs	5.0	All	All	All
Application	Cisco	Crs	6.0	All	All	All
Application	Cisco	Crs	7.0	All	All	All
Application	Cisco	Customer Response Applications	3.5	All	All	All
Application	Cisco	Customer Response Applications	3.5	All	All	All
Application	Cisco	Ip Qm	3.5	All	All	All

Application	Cisco	Ip Qm	3.5	All	All	All
Application	Cisco	Unified Ccx	3.5	All	All	All
Application	Cisco	Unified Ccx	4.0(1)	All	All	All
Application	Cisco	Unified Ccx	4.0(3)	All	All	All
Application	Cisco	Unified Ccx	4.0(4)	All	All	All
Application	Cisco	Unified Ccx	4.0(5)	All	All	All
Application	Cisco	Unified Ccx	4.0(5a)	All	All	All
Application	Cisco	Unified Ccx	4.0(1)	All	All	All
Application	Cisco	Unified Ccx	4.0(3)	All	All	All
Application	Cisco	Unified Ccx	4.0(4)	All	All	All
Application	Cisco	Unified Ccx	4.0(5a)	All	All	All
Application	Cisco	Unified Ccx	4.0(5)	All	All	All
Application	Cisco	Unified Ccx	4.5(1)	All	All	All
Application	Cisco	Unified Ccx	4.5(2)	All	All	All
Application	Cisco	Unified Ccx	4.5(1)	All	All	All
Application	Cisco	Unified Ccx	4.5(2)	All	All	All
Application	Cisco	Unified Ccx	5.0(1)	All	All	All
Application	Cisco	Unified Ccx	5.0(1)	All	All	All
Application	Cisco	Unified Ccx	6.0(1)	All	All	All
Application	Cisco	Unified Ccx	6.0(1)	All	All	All
Application	Cisco	Unified Ccx	7.0(1)	All	All	All
Application	Cisco	Unified Ccx	7.0(1)	All	All	All
Application	Cisco	Unified Ccx	3.5	All	All	All
Application	Cisco	Unified Ccx	4.0(1)	All	All	All
Application	Cisco	Unified Ccx	4.0(3)	All	All	All
Application	Cisco	Unified Ccx	4.0(4)	All	All	All
Application	Cisco	Unified Ccx	4.0(5a)	All	All	All
Application	Cisco	Unified Ccx	4.0(5)	All	All	All
Application	Cisco	Unified Ccx	4.5(1)	All	All	All
Application	Cisco	Unified Ccx	4.5(2)	All	All	All
Application	Cisco	Unified Ccx	5.0(1)	All	All	All
Application	Cisco	Unified Ccx	6.0(1)	All	All	All
Application	Cisco	Unified Ccx	7.0(1)	All	All	All
Application	Cisco	Unified Ip Contact Center Express	3.0	All	All	All
Application	Cisco	Unified Ip Contact Center Express	5.0(1)	All	All	All

Application	Cisco	Unified Ip Contact Center Express	5.0(1\)	All	All	All
Application	Cisco	Unified Ip Contact Center Express	6.0(1)	All	All	All
Application	Cisco	Unified Ip Contact Center Express	6.0(1\)	All	All	All
Application	Cisco	Unified Ip Contact Center Express	7.0	All	All	All
Application	Cisco	Unified Ip Contact Center Express	3.0	All	All	All
Application	Cisco	Unified Ip Contact Center Express	5.0(1\)	All	All	All
Application	Cisco	Unified Ip Contact Center Express	6.0(1\)	All	All	All
Application	Cisco	Unified Ip Contact Center Express	7.0	All	All	All
Application	Cisco	Unified Ip lvr	3.0	All	All	All
Application	Cisco	Unified Ip lvr	3.1	All	All	All
Application	Cisco	Unified Ip lvr	4.0	All	All	All
Application	Cisco	Unified Ip lvr	4.1	All	All	All
Application	Cisco	Unified Ip lvr	4.5	All	All	All
Application	Cisco	Unified Ip lvr	5.0	All	All	All
Application	Cisco	Unified Ip lvr	6.0	All	All	All
Application	Cisco	Unified Ip lvr	7.0	All	All	All
Application	Cisco	Unified Ip lvr	7.0(1)	All	All	All
Application	Cisco	Unified Ip lvr	7.0(1\)	All	All	All
Application	Cisco	Unified Ip lvr	3.0	All	All	All
Application	Cisco	Unified Ip lvr	3.1	All	All	All
Application	Cisco	Unified Ip lvr	4.0	All	All	All
Application	Cisco	Unified Ip lvr	4.1	All	All	All
Application	Cisco	Unified Ip lvr	4.5	All	All	All
Application	Cisco	Unified Ip lvr	5.0	All	All	All
Application	Cisco	Unified Ip lvr	6.0	All	All	All
Application	Cisco	Unified Ip lvr	7.0	All	All	All
Application	Cisco	Unified Ip lvr	7.0(1\)	All	All	All

References

Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Cisco Security Advisory: Vulnerabilities in Unified Contact Center Express Administration Pages - Cisco Systems

55936

Cisco Unified Contact Center Express Two Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

Cisco Unified Contact Center Express Express Administration Pages Permit Script Injection and Directory Traversal Attacks - SecurityTracker

IBM X-Force Exchange

Cisco Unified Contact Center Express CRS Administration Interface Directory Traversal Vulnerability

CVE Program record

NVD vulnerability detail



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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)