CVE-2002-0778

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2002-0778
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-08-12 04:00:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	The default configuration of the proxy for Cisco Cache Engine and Content Engine allows remote attackers to use HTTPS t

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Cache Engine 505	2.4.0	All	All	All
Hardware	Cisco	Cache Engine 505	3.0	All	All	All
Hardware	Cisco	Cache Engine 505	2.4.0	All	All	All
Hardware	Cisco	Cache Engine 505	3.0	All	All	All
Hardware	Cisco	Cache Engine 550	All	All	All	All
Hardware	Cisco	Cache Engine 550	2.2.0	All	All	All
Hardware	Cisco	Cache Engine 550	2.4.0	All	All	All
Hardware	Cisco	Cache Engine 550	3.0	All	All	All
Hardware	Cisco	Cache Engine 550	All	All	All	All
Hardware	Cisco	Cache Engine 550	2.2.0	All	All	All
Hardware	Cisco	Cache Engine 550	2.4.0	All	All	All
Hardware	Cisco	Cache Engine 550	3.0	All	All	All
Hardware	Cisco	Cache Engine 570	2.2.0	All	All	All
Hardware	Cisco	Cache Engine 570	2.4.0	All	All	All
Hardware	Cisco	Cache Engine 570	3.0	All	All	All
Hardware	Cisco	Cache Engine 570	570	All	All	All
Hardware	Cisco	Cache Engine 570	2.2.0	All	All	All

Hardware	Cisco	Cache Engine 570	2.4.0	All	All	All
Hardware	Cisco	Cache Engine 570	3.0	All	All	All
Hardware	Cisco	Cache Engine 570	570	All	All	All
Application	Cisco	Content Distribution Manager 4630	All	All	All	All
Application	Cisco	Content Distribution Manager 4630	4.0	All	All	All
Application	Cisco	Content Distribution Manager 4630	4.1	All	All	All
Application	Cisco	Content Distribution Manager 4630	All	All	All	All
Application	Cisco	Content Distribution Manager 4630	4.0	All	All	All
Application	Cisco	Content Distribution Manager 4630	4.1	All	All	All
Application	Cisco	Content Distribution Manager 4650	All	All	All	All
Application	Cisco	Content Distribution Manager 4650	4.0	All	All	All
Application	Cisco	Content Distribution Manager 4650	4.1	All	All	All
Application	Cisco	Content Distribution Manager 4650	All	All	All	All
Application	Cisco	Content Distribution Manager 4650	4.0	All	All	All
Application	Cisco	Content Distribution Manager 4650	4.1	All	All	All
Application	Cisco	Content Engine	507	All	All	All
Application	Cisco	Content Engine	507_2.2.0	All	All	All
Application	Cisco	Content Engine	507_3.1	All	All	All
Application	Cisco	Content Engine	507_4.0	All	All	All
Application	Cisco	Content Engine	507_4.1	All	All	All
Application	Cisco	Content Engine	560	All	All	All
Application	Cisco	Content Engine	560_2.2.0	All	All	All
Application	Cisco	Content Engine	560_3.1	All	All	All
Application	Cisco	Content Engine	560_4.0	All	All	All
Application	Cisco	Content Engine	560_4.1	All	All	All
Application	Cisco	Content Engine	590	All	All	All
Application	Cisco	Content Engine	590_2.2.0	All	All	All
Application	Cisco	Content Engine	590_3.1	All	All	All
Application	Cisco	Content Engine	590_4.0	All	All	All
Application	Cisco	Content Engine	590_4.1	All	All	All
Application	Cisco	Content Engine	7320	All	All	All
Application	Cisco	Content Engine	7320_2.2.0	All	All	All
Application	Cisco	Content Engine	7320_3.1	All	All	All
Application	Cisco	Content Engine	7320_4.0	All	All	All
Application	Cisco	Content Engine	7320_4.1	All	All	All

Application	Cisco	Content Engine	507	All	All	All
Application	Cisco	Content Engine	507_2.2.0	All	All	All
Application	Cisco	Content Engine	507_3.1	All	All	All
Application	Cisco	Content Engine	507_4.0	All	All	All
Application	Cisco	Content Engine	507_4.1	All	All	All
Application	Cisco	Content Engine	560	All	All	All
Application	Cisco	Content Engine	560_2.2.0	All	All	All
Application	Cisco	Content Engine	560_3.1	All	All	All
Application	Cisco	Content Engine	560_4.0	All	All	All
Application	Cisco	Content Engine	560_4.1	All	All	All
Application	Cisco	Content Engine	590	All	All	All
Application	Cisco	Content Engine	590_2.2.0	All	All	All
Application	Cisco	Content Engine	590_3.1	All	All	All
Application	Cisco	Content Engine	590_4.0	All	All	All
Application	Cisco	Content Engine	590_4.1	All	All	All
Application	Cisco	Content Engine	7320	All	All	All
Application	Cisco	Content Engine	7320_2.2.0	All	All	All
Application	Cisco	Content Engine	7320_3.1	All	All	All
Application	Cisco	Content Engine	7320_4.0	All	All	All
Application	Cisco	Content Engine	7320_4.1	All	All	All
Hardware	Cisco	Content Router 4430	All	All	All	All
Hardware	Cisco	Content Router 4430	All	All	All	All
Application	Cisco	Enterprise Content Delivery Network Software	4.0	All	All	All
Application	Cisco	Enterprise Content Delivery Network Software	4.1	All	All	All
Application	Cisco	Enterprise Content Delivery Network Software	4.0	All	All	All
Application	Cisco	Enterprise Content Delivery Network Software	4.1	All	All	All

References

Reference
Cisco Security Advisory: Transparent Cache Engine and Content Engine TCP Relay Vulnerability
ISS X-Force Database: cisco-cache-content-tcp-forward (9082): Cisco Cache and Content Engines could allow an attacker to spoof the origin
Cisco Cache Engine Default Configuration Arbitrary User Proxy Vulnerability
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this 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 registred 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