



CVE-2010-3036

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

Summary

CVE	CVE-2010-3036
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-10-29 19:00:00 UTC
Updated	2010-11-06 05:38:00 UTC
Description	Multiple buffer overflows in the authentication functionality in the web-server module in Cisco CiscoWorks Common Service

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ciscoverks Common Services	3.0.5	All	All	All
Application	Cisco	Ciscoverks Common Services	3.0.6	All	All	All
Application	Cisco	Ciscoverks Common Services	3.1	All	All	All
Application	Cisco	Ciscoverks Common Services	3.1.1	All	All	All
Application	Cisco	Ciscoverks Common Services	3.2	All	All	All
Application	Cisco	Ciscoverks Common Services	3.3	All	All	All
Application	Cisco	Ciscoverks Common Services	3.0.5	All	All	All
Application	Cisco	Ciscoverks Common Services	3.0.6	All	All	All
Application	Cisco	Ciscoverks Common Services	3.1	All	All	All
Application	Cisco	Ciscoverks Common Services	3.1.1	All	All	All
Application	Cisco	Ciscoverks Common Services	3.2	All	All	All
Application	Cisco	Ciscoverks Common Services	3.3	All	All	All
Application	Cisco	Ciscoverks Lan Management Solution	2.6	update	All	All
Application	Cisco	Ciscoverks Lan Management Solution	3.0	All	All	All
Application	Cisco	Ciscoverks Lan Management Solution	3.0	december_2007	All	All
Application	Cisco	Ciscoverks Lan Management Solution	3.1	All	All	All
Application	Cisco	Ciscoverks Lan Management Solution	3.2	All	All	All

Application	Cisco	Ciscoworks Lan Management Solution	2.6	update	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.0	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.0	december_2007	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.1	All	All	All
Application	Cisco	Ciscoworks Lan Management Solution	3.2	All	All	All
Application	Cisco	Qos Policy Manager	4.0	All	All	All
Application	Cisco	Qos Policy Manager	4.0.1	All	All	All
Application	Cisco	Qos Policy Manager	4.0.2	All	All	All
Application	Cisco	Qos Policy Manager	4.0	All	All	All
Application	Cisco	Qos Policy Manager	4.0.1	All	All	All
Application	Cisco	Qos Policy Manager	4.0.2	All	All	All
Application	Cisco	Security Manager	3.0.2	All	All	All
Application	Cisco	Security Manager	3.2	All	All	All
Application	Cisco	Security Manager	3.0.2	All	All	All
Application	Cisco	Security Manager	3.2	All	All	All
Application	Cisco	Telepresence Readiness Assessment Manager	1.0	All	All	All
Application	Cisco	Telepresence Readiness Assessment Manager	1.0	All	All	All
Application	Cisco	Unified Operations Manager	2.0.1	All	All	All
Application	Cisco	Unified Operations Manager	2.0.2	All	All	All
Application	Cisco	Unified Operations Manager	2.0.3	All	All	All
Application	Cisco	Unified Operations Manager	2.0.1	All	All	All
Application	Cisco	Unified Operations Manager	2.0.2	All	All	All
Application	Cisco	Unified Operations Manager	2.0.3	All	All	All
Application	Cisco	Unified Service Monitor	2.0.1	All	All	All
Application	Cisco	Unified Service Monitor	2.0.1	All	All	All

References

Reference	Source
SecurityTracker.com Archives - CiscoWorks Common Services Buffer Overflow Lets Remote Users Execute Arbitrary Code	SECTRACK
68927	OSVDB
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
Cisco Security Advisory: CiscoWorks Common Services Arbitrary Code Execution Vulnerability - Cisco Systems	CISCO
CiscoWorks Common Services Buffer Overflow Vulnerability - Advisories - Community	SECUNIA
Cisco CiscoWorks Common Services Web Server Module Buffer Overflow Vulnerability	BID
CVE Program record	CVE.ORG

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](#)