



CVE-2006-5571

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

Summary

CVE	CVE-2006-5571
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-27 16:07:00 UTC
Updated	2018-10-17 21:43:00 UTC
Description	Stack-based buffer overflow in /scripts/cruise/cws.exe in CruiseWorks 1.09c and 1.09d allows remote attackers to execute a

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Kynoslogic	Cruiseworks	1.09c	All	All	All
Application	Kynoslogic	Cruiseworks	1.09d	All	All	All
Application	Kynoslogic	Cruiseworks	1.09c	All	All	All
Application	Kynoslogic	Cruiseworks	1.09d	All	All	All

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
SecurityTracker.com Archives - CruiseWorks 'cws.exe' Input Validation Errors Let Remote Users Traverse the Directory or Execute Arbitrary C
[vuln.sg] CruiseWorks Directory Traversal and Buffer Overflow Vulnerabilities
'[Full-disclosure] [vuln.sg] CruiseWorks Directory Traversal and' - MARC
SecurityFocus
IBM X-Force Exchange
CruiseWorks Directory Traversal and Buffer Overflow Vulnerabilities - Advisories - Secunia
CruiseWorks Directory Traversal and Buffer Overflow Vulnerabilities - CXSecurity.com
Cruiseworks Cws.exe Doc Buffer Overflow Vulnerability
CVE Program record

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](#)