



CVE-2006-1961

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

Summary

CVE	CVE-2006-1961
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-04-21 10:02:00 UTC
Updated	2018-10-18 16:37:00 UTC
Description	Cisco CiscoWorks Wireless LAN Solution Engine (WLSE) and WLSE Express before 2.13, Hosting Solution Engine (HSE)

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ciscoworks 2000 Service Management Solution	All	All	All	All
Application	Cisco	Ciscoworks 2000 Service Management Solution	All	All	All	All
Operating System	Cisco	Ethernet Subscriber Solution Engine	All	All	All	All
Operating System	Cisco	Ethernet Subscriber Solution Engine	All	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.0	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.1	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.2	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.3	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.0	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.1	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.2	All	All	All
Hardware	Cisco	Hosting Solution Engine	1.7.3	All	All	All
Application	Cisco	User Registration Tool	All	All	All	All
Application	Cisco	User Registration Tool	All	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.0	All	All	All

Application	Cisco	Wireless Lan Solution Engine	2.12	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.12	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.13	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.13	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.2	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.2	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.3	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.3	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.4	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.4	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.5	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.5	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.6	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.6	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.7	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.7	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.8	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.8	All	express	All
Application	Cisco	Wireless Lan Solution Engine	2.9	All	All	All
Application	Cisco	Wireless Lan Solution Engine	2.9	All	express	All

References

Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

CiscoWorks Wireless LAN Solution Engine Cross-Site Scripting Flaw Yields Administrative Privileges and Command Line Bug Lets Remote A

24813

Multiple Linux-Based Cisco Products Local Privilege Escalation Vulnerability

SecurityFocus

IBM X-Force Exchange

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityFocus

Cisco Hosting Solution Engine / User Registration Tool Privilege Escalation - Advisories - Secunia

Page not found - CyberCX | Australia

Cisco WLSE Privilege Escalation and Cross-Site Scripting - Advisories - Secunia

Cisco - Networking, Cloud, and Cybersecurity Solutions

Cisco ESSE / SMS Privilege Escalation Vulnerability - Advisories - Secunia

Cisco - Networking, Cloud, and Cybersecurity Solutions

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](#)