



CVE-2014-0673

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

Summary

CVE	CVE-2014-0673
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-25 22:55:03 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the web interface on Cisco Video Surveillance 5000 HD IP Dome camer

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

EPSS: 0.005430000 probability, percentile 0.677990000 (date 2026-05-03)

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Hardware	Cisco	Video Surveillance Indoor Fixed Dome Ip Hd Camera	5010	All	All	All
Hardware	Cisco	Video Surveillance Indoor Fixed Dome Ip Hd Camera	5011	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Security Advisory SA56552 - Cisco Video Surveillance 5000 Series HD IP Dome Camera Two Cross-Site Scripting Vulnerabilities - Secunia
IBM X-Force Exchange
Cisco Video Surveillance 5000 Series IP Dome Cameras Multiple Cross Site Scripting Vulnerabilities
Alert Details - Security Center - Cisco Systems
Cisco Video Surveillance Camera Input Validation Hole Permits Cross-Site Scripting Attacks - SecurityTracker
Cisco Security Notice: Cisco Video Surveillance 5000 Series HD IP Dome Camera Multiple Cross-Site Scripting Vulnerabilities
osvdb.org/102557
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.