



CVE-2015-0577

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

Summary

CVE	CVE-2015-0577
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-14 19:59:01 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in the IronPort Spam Quarantine (ISQ) page in Cisco AsyncOS, as used o

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

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
Operating System	Cisco	Asyncos	-	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				Sou
Security Advisory SA62289 - Cisco IronPort AsyncOS Cross-Site Scripting Vulnerabilities - Secunia				af85
Malformed Request				af85
Cisco Email Security Appliance Input Validation Flaw in Spam Quarantine Page Permits Cross-Site Scripting Attacks - SecurityTracker				af85
IBM X-Force Exchange				af85
Cisco AsyncOS ISQ XSS Vulnerability				af85
CVE Program record				CVE
NVD vulnerability detail				NVD
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				