



CVE-2014-3821

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

Summary

CVE	CVE-2014-3821
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-11 20:55:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in SRX Web Authentication (webauth) in Juniper Junos 11.4 before 11.4R11, 12.1X

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	Juniper	Junos	11.4	All	All	All

Operating System	Juniper	Junos	12.1x44	All	All	All
Operating System	Juniper	Junos	12.1x45	All	All	All
Operating System	Juniper	Junos	12.1x46	All	All	All
Operating System	Juniper	Junos	12.1x47	All	All	All

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

References
Reference
Juniper Junos SRX Web Authentication Cross Site Scripting Vulnerability
Juniper Networks - 2014-07 Security Bulletin: Junos: XSS vulnerability in web authentication (webauth) (CVE-2014-3821) - Knowledge Base
Juniper Junos SRX Input Validation Flaw in Web Authentication Permits Cross-Site Scripting Attacks - SecurityTracker
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.