



# CVE-2014-2120

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2014-2120
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisco
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-03-19 01:15:04 UTC
<b>Updated</b>	2026-04-21 18:07:39 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in the WebVPN login page in Cisco Adaptive Security Appliance (ASA) Software allc

## Risk And Classification

**Primary CVSS:** v3.1 6.1 MEDIUM from nvd@nist.gov

**CVSS:** 3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

**EPSS:** 0.698380000 probability, percentile 0.986770000 (date 2026-04-26)

**CISA KEV:** Listed on 2024-11-12; due 2024-12-03; ransomware use Unknown

**Problem Types:** CWE-79 | n/a | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	ADP	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
2.0	nvd@nist.gov	Primary	4.3		AV:N/AC:M/Au:N/C:N/I:P/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

### 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

### CISA Known Exploited Vulnerability

<b>Vendor</b>	Cisco
<b>Product</b>	Adaptive Security Appliance (ASA)
<b>Name</b>	Cisco Adaptive Security Appliance (ASA) Cross-Site Scripting (XSS) Vulnerability
<b>Required Action</b>	Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.
<b>Notes</b>	<a href="https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CVE-2014-2120">https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CVE-2014-2120</a> ; <a href="https://nvd.nist.gov/vuln/detail/CVE-2014-2120">https://nvd.nist.gov/vuln/detail/CVE-2014-2120</a>

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Adaptive Security Appliance Software	-	All	All	All

### Vendor Declared Affected Products

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

ADP	Cisco	Adaptive Security Appliance Software	affected * custom	Not specified
References				
Reference	Source			
Cisco ASA Input Validation Hole in WebVPN Interface Permits Cross-Site Scripting Attacks - SecurityTracker	af854a3a-2127-422b-91a6			
Cisco Adaptive Security Appliance CVE-2014-2120 Cross Site Scripting Vulnerability	af854a3a-2127-422b-91a6			
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3			
Cisco Security Notice: Cisco Adaptive Security Appliance WebVPN Login Page Cross-Site Scripting Vulnerability	af854a3a-2127-422b-91a6			
CVE Program record	CVE.ORG			
NVD vulnerability detail	NVD			
CISA Known Exploited Vulnerabilities catalog	CISA			
No vendor comments have been submitted for this CVE.				
Additional Advisory Data				
Source	Time	Event		
ADP	2024-11-12T00:00:00.000Z	CVE-2014-2120 added to CISA KEV		
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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)