

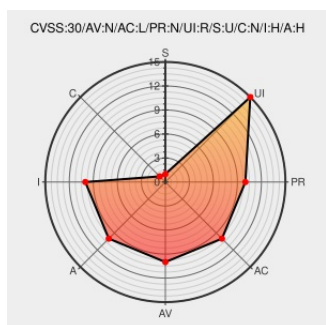


CVE-2019-1713

Published on: 05/03/2019 12:00:00 AM UTC

Last Modified on: 08/15/2023 03:24:00 PM UTC

CVE-2019-1713 - advisory for cisco-sa-20190501-asa-csrf

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Adaptive Security Appliance Software](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management

interface on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. If the user has administrative privileges, the attacker could alter the configuration of, extract information from, or reload an affected device.

CVE-2019-1713 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Adaptive Security Appliance (ASA) Software version 9.4.4.34**

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Adaptive Security Appliance (ASA) Software version 9.6.4.25**

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Adaptive Security Appliance (ASA) Software version 9.8.4**

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Adaptive Security Appliance (ASA) Software version 9.9.2.50**

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Adaptive Security Appliance (ASA) Software version 9.10.1.17**

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact

UNCHANGED		HIGH		HIGH		HIGH	
CVSS2 Score: 9.3 - HIGH							
Access Vector		Access Complexity		Authentication			
NETWORK		MEDIUM		NONE			
Confidentiality Impact		Integrity Impact		Availability Impact			
COMPLETE		COMPLETE		COMPLETE			
CVE References							
Description		Tags		Link			
Cisco Adaptive Security Appliance Software Cross-Site Request Forgery Vulnerability		Vendor Advisory tools.cisco.com text/html		CISCO 20190501 Cisco Adaptive Security Appliance Software Cross-Site Request Forgery Vulnerability			
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.							
There are currently no QIDs associated with this CVE							
Known Affected Configurations (CPE V2.3)							
Type	Vendor	Product		Version	Update	Edition	Language
Application	Cisco	Adaptive Security Appliance Software		All	All	All	All
Operating System	Cisco	Adaptive Security Appliance Software		All	All	All	All
Application	Cisco	Adaptive Security Appliance Software		All	All	All	All
Hardware 	Cisco	Asa 5505		-	All	All	All
Hardware 	Cisco	Asa 5505		-	All	All	All
Hardware 	Cisco	Asa 5510		-	All	All	All
Hardware 	Cisco	Asa 5510		-	All	All	All
Hardware 	Cisco	Asa 5512-x		-	All	All	All
Hardware 	Cisco	Asa 5512-x		-	All	All	All
Hardware 	Cisco	Asa 5515-x		-	All	All	All
Hardware 	Cisco	Asa 5515-x		-	All	All	All
Hardware 	Cisco	Asa 5520		-	All	All	All
Hardware 	Cisco	Asa 5520		-	All	All	All
Hardware 	Cisco	Asa 5525-x		-	All	All	All

Hardware  	Cisco	Asa 5525-x	-	All	All	All
Hardware  	Cisco	Asa 5540	-	All	All	All
Hardware  	Cisco	Asa 5540	-	All	All	All
Hardware  	Cisco	Asa 5545-x	-	All	All	All
Hardware  	Cisco	Asa 5545-x	-	All	All	All
Hardware  	Cisco	Asa 5550	-	All	All	All
Hardware  	Cisco	Asa 5550	-	All	All	All
Hardware  	Cisco	Asa 5555-x	-	All	All	All
Hardware  	Cisco	Asa 5555-x	-	All	All	All
Hardware  	Cisco	Asa 5580	-	All	All	All
Hardware  	Cisco	Asa 5580	-	All	All	All
Hardware  	Cisco	Asa 5585-x	-	All	All	All
Hardware  	Cisco	Asa 5585-x	-	All	All	All

```
cpe:2.3:a:cisco:adaptive_security_appliance_software:*:*:*:*:*.*
```

```
cpe:2.3:o:cisco:adaptive_security_appliance_software:*:*:*:*:*.*
```

```
cpe:2.3:a:cisco:adaptive_security_appliance_software:.*:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:h:cisco:asa_5505:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5505:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5510:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5510:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5512-x:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5512-x:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5515-x:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5515-x:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5520:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5520:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5525-x:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa_5525-x:-:*:*:*:*:*:
```

```
cpe:2.3:h:cisco:asa 5540:-:*:*:*:*:*:*:
```

cpe:2.3:h:cisco:asa_5540:-:*****:
cpe:2.3:h:cisco:asa_5545-x:-:*****:
cpe:2.3:h:cisco:asa_5545-x:-:*****:
cpe:2.3:h:cisco:asa_5550:-:*****:
cpe:2.3:h:cisco:asa_5550:-:*****:
cpe:2.3:h:cisco:asa_5555-x:-:*****:
cpe:2.3:h:cisco:asa_5555-x:-:*****:
cpe:2.3:h:cisco:asa_5580:-:*****:
cpe:2.3:h:cisco:asa_5580:-:*****:
cpe:2.3:h:cisco:asa_5585-x:-:*****:
cpe:2.3:h:cisco:asa_5585-x:-:*****:

No vendor comments have been submitted for this CVE