



CVE-2014-3399

Published on: 10/07/2014 12:00:00 AM UTC

Last Modified on: 06/02/2022 03:47:00 PM UTC

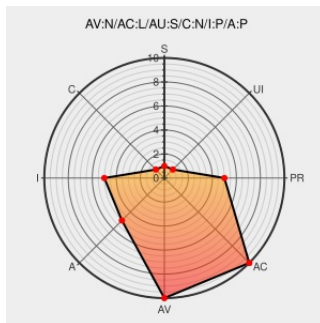
CVE-2014-3399

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The SSL VPN implementation in Cisco Adaptive Security Appliance (ASA) Software 9.2(.2.4) and earlier does not properly manage session information during creation of a SharePoint handler, which allows remote authenticated users to overwrite arbitrary RAMFS cache files or inject Lua programs, and consequently cause a denial of service (portal outage or system reload), via crafted HTTP requests, aka Bug ID CSCup54208.

CVE-2014-3399 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
No Description Provided	Vendor Advisory tools.cisco.com text/html	CISCO 20141006 Cisco ASA Software SharePoint RAMFS Integrity and Lua Injection Vulnerability
No Description Provided	Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/viewAlert.x?alertId=35989

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	9.1	All	All	All
Application	Cisco	Adaptive Security Appliance Software	9.1	All	All	All
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All
Application	Cisco	Adaptive Security Appliance Software	All	All	All	All

```
cpe:2.3:a:cisco:adaptive_security_appliance_software:9.1:::*:*:*:
```

```
cpe:2.3:a:cisco:adaptive_security_appliance_software:9.1:::*:*:*:
```

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

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

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status status.cve.report