

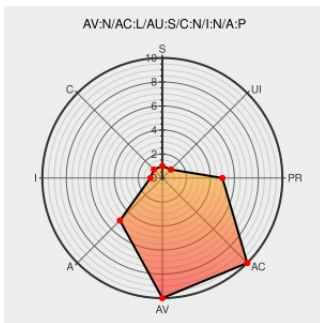


CVE-2014-3276

Published on: 05/23/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:47 PM UTC

CVE-2014-3276

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

Certain versions of [Identity Services Engine Software](#) from [Cisco](#) contain the following vulnerability:

Cisco Identity Services Engine (ISE) 1.2(.1 patch 2) and earlier does not properly handle deadlock conditions during reception of crafted RADIUS accounting packets from multiple NAS devices, which allows remote authenticated users to cause a denial of service (RADIUS outage) by sourcing these packets from two origins, aka Bug ID

CSCuo56780.

CVE-2014-3276 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

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

CVE References

Description	Tags	Link
Cisco Security Notice: Cisco ISE RADIUS Service Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20140521 Cisco ISE RADIUS Service Denial of Service Vulnerability
Alert Details - Security Center - Cisco Systems	Vendor Advisory tools.cisco.com text/html	CONFIRM tools.cisco.com/security/center/viewAlert.x?alertId=34329
Cisco Identity Services Engine RADIUS Processing Flaw Lets Remote Authenticated Users Deny Service - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRAK 1030274

By selecting these links, you may be leaving CVEreport webpage. We have provided these links to other websites because they may have information that

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	Identity Services Engine Software	1.0	All	All	All
Application	Cisco	Identity Services Engine Software	1.1	All	All	All
Application	Cisco	Identity Services Engine Software	1.0	All	All	All
Application	Cisco	Identity Services Engine Software	1.1	All	All	All
Application	Cisco	Identity Services Engine Software	All	All	All	All
cpe:2.3:a:cisco:identity_services_engine_software:1.0:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine_software:1.1:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine_software:1.0:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine_software:1.1:*:*:*:*:*:						
cpe:2.3:a:cisco:identity_services_engine_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](#)