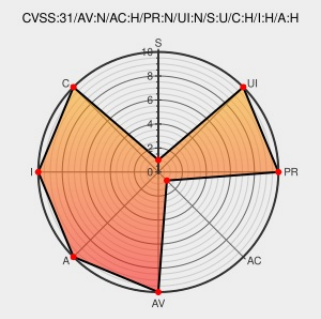
CVE-2017-10873

Published on: 11/02/2017 12:00:00 AM UTC

Last Modified on: 09/09/2021 12:58:00 PM UTC

CVE-2017-10873

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openam from Open Source Solution Technology contain the following vulnerability:

OpenAM (Open Source Edition) allows an attacker to bypass authentication and access unauthorized contents via unspecified vectors. Note that this vulnerability affects OpenAM (Open Source Edition) implementations configured as SAML 2.0IdP, and switches authentication methods based on AuthnContext requests sent from the service provider.

CVE-2017-10873 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Open Source Solution Technology Corporation** - **OpenAM** version **Open Source Edition**

CVSS3 Score: 8.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

Notice of OpenAM security vulnerability and product updates [AM20171101-1] - Open Source Solution Technology Corporation	Patch Vendor Advisory www.osstech.co.jp text/html	MISC www.osstech.co.jp/support/am2017-2-1-en
JVN#79546124: OpenAM (Open Source Edition) vulnerable to authentication bypass	Third Party Advisory VDB Entry jvn.jp text/xml	JVN JVN#97243511
ThemiStruct サポートサイト	Third Party Advisory www.cs.themistruct.com text/html	MISC www.cs.themistruct.com/

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	Open Source Solution Technology	Openam	All	All	All	All
Application	Open Source Solution Technology	Openam	All	All	All	All
Application	Open Source Solution Technology	Openam	All	All	All	All
Application	Osstech	Openam	All	All	All	All
Application	Osstech	Openam	All	All	All	All
Application	Osstech	Openam	All	All	All	All

cpe:2.3:a:open_source_solution_technology:openam:*:*:*:*:open_source:*:*:*:

cpe:2.3:a:open_source_solution_technology:openam:*:*:*:*:open_source:*:*:*:

cpe:2.3:a:open_source_solution_technology:openam:*:*:*:*:open_source:*:*:*:

cpe:2.3:a:osstech:openam:*:*:*:*:open_source:*:*:*:

cpe:2.3:a:osstech:openam:*:*:*:*:open_source:*:*:*:

cpe:2.3:a:osstech:openam:*:*:*:*:open_source:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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