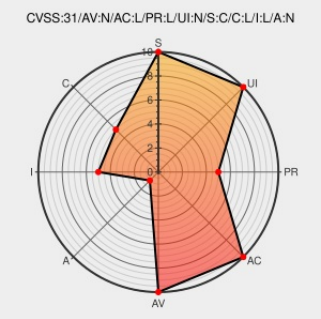
CVE-2021-34706

Published on: 10/06/2021 12:00:00 AM UTC

Last Modified on: 10/14/2021 09:14:00 PM UTC

CVE-2021-34706 - advisory for cisco-sa-ise-xxe-inj-V4VSjEsX

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



Certain versions of Identity Services Engine from Cisco contain the following vulnerability:

A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access sensitive information or conduct a server-side request forgery (SSRF) attack through an affected device. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of sensitive information, or cause the web application to perform arbitrary HTTP requests on behalf of the attacker.

CVE-2021-34706 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco 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 Identity Services Engine Software** version **n/a**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Cisco Identity Services Engine XML External Entity Injection Vulnerability	tools.cisco.com text/html	CISCO 20211006 Cisco Identity Services Engine XML External Entity Injection 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.

Related QID Numbers

317070 Cisco Identity Services Engine (ISE) Extensible Markup Language (XML) External Entity Injection Vulnerability (cisco-sa-ise-xxe-inj-V4VSjEsX)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine	3.1\(0.518\)	All	All	All
Application	Cisco	Identity Services Engine	3.2\(0.149\)	All	All	All
Application	Cisco	Identity Services Engine	All	All	All	All

cpe:2.3:a:cisco:identity_services_engine:3.1\(0.518\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:3.2\(0.149\):*:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-34706 : A vulnerability in the web-based management interface of Cisco Identity Services Engine ISE co… twitter.com/i/web/status/1…	2021-10-06 20:01:02
@softek_jp	Cisco ISE Software の Web 管理インターフェイスの処理にサーバサイドリクエストフォージェリの問題 (CVE-2021-34706 [40168] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-10-07 05:14:36

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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