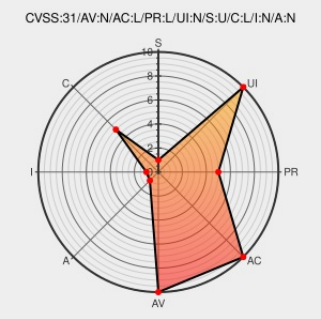
CVE-2021-34702

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

Last Modified on: 11/07/2023 03:36:00 AM UTC

CVE-2021-34702 - advisory for cisco-sa-ise-info-disc-pNXtLhdp

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 obtain sensitive information. This vulnerability is due to improper enforcement of administrator privilege levels for low-value sensitive data. An attacker with read-only administrator access to the web-based management interface could exploit this vulnerability by browsing to the page that contains the sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system.

CVE-2021-34702 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: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability	tools.cisco.com text/html	CISCO 20211006 Cisco Identity Services Engine Sensitive Information Disclosure Vulnerability

Related QID Numbers

317071 Cisco Identity Services Engine (ISE) Sensitive Information Disclosure Vulnerability (cisco-sa-ise-info-disc-pNXtLhdp)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine	All	All	All	All
Application	Cisco	Identity Services Engine	2.6.0	-	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch1	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch10	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch2	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch3	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch5	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch6	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch7	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch8	All	All
Application	Cisco	Identity Services Engine	2.6.0	patch9	All	All
Application	Cisco	Identity Services Engine	2.7.0	-	All	All
Application	Cisco	Identity Services Engine	2.7.0	patch1	All	All
Application	Cisco	Identity Services Engine	2.7.0	patch2	All	All
Application	Cisco	Identity Services Engine	2.7.0	patch3	All	All
Application	Cisco	Identity Services Engine	2.7.0	patch4	All	All
Application	Cisco	Identity Services Engine	3.0.0	-	All	All
Application	Cisco	Identity Services Engine	3.0.0	patch1	All	All
Application	Cisco	Identity Services Engine	3.0.0	patch2	All	All
Application	Cisco	Identity Services Engine	3.0.0	patch3	All	All

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

cpe:2.3:a:cisco:identity_services_engine:2.6.0:-:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch1:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch10:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch2:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch3:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch5:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch6:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch7:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch8:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.6.0:patch9:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.7.0:-:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch1:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch2:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch3:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:2.7.0:patch4:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:3.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:3.0.0:patch1:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:3.0.0:patch2:*:*:*:*:*:*:

cpe:2.3:a:cisco:identity_services_engine:3.0.0:patch3:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-34702 : A vulnerability in the web-based management interface of Cisco Identity Services Engine ISE co… twitter.com/i/web/status/1…	2021-10-06 20:00:37
@softek_jp	Cisco ISE Software の Web 管理インターフェイスの処理に情報漏洩の問題 (CVE-2021-34702) [40166] sid.softek.jp/content/show/4… #SIDfm #脆弱性情報	2021-10-07 05:14:35

← Previous ID

Next ID→

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