

Cisco Identity Services

Engine (ISE) Web UI - Authentication bypass



Cisco Identity Services (ISE) Web UI - Authentication bypass (CVE-2022-20782)

Severity: Medium

Published: 2022-04-06 16:00

Version: ISE 1.0 : Final

CVSS Score: 6.5

Workarounds: No workarounds available

Cisco ID: CSCvz20851

Authentication bypass in Cisco Identity Services (ISE) Web UI

Summary

Cisco Identity Services

Engine (ISE) Web UI - Authentication bypass (CVE-2022-20782)

This vulnerability allows an attacker to bypass authentication in the Cisco Identity Services (ISE) Web UI.

The attack is performed by sending a specially crafted request to the ISE Web UI, which results in the user being authenticated without providing valid credentials.

For more information, see the Cisco Security Advisory at <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s>.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s>

Impact

Authentication bypass, Denial of Service

The impact of this vulnerability is that an attacker can bypass authentication in the Cisco Identity Services (ISE) Web UI.

This could result in unauthorized access to sensitive information and the ability to perform administrative actions.

The severity of this vulnerability is Medium (CVSS 6.5).

Workarounds: There are no workarounds available for this vulnerability.

References: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s>

For more information, see the Cisco Security Advisory at <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s>.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s>

Product Security Incident Response Team (PSIRT);

af—afaf€ä, -af^ ä, »ä, af¥af^af†ä, f

ä, af^3ä, .af†af^3af^ af-ä, 1af äf^3ä, 1

ä, æfå^©ç''' ä°<ä¾<ä ä " ä...-å¼ç™°èi''

Cisco PSIRT

ä s ä -ä€ äœ-ä, çäf%ä f ä, ä, ¶ä, ¶ä f ä «è ~ è¼%ä ä •ä, Cä | ä ,, ä, <è, †å¼±æfSä ®ä, æfå^©ç

å†°å... ,

æœ-è, , †å¼±æ€šä -ä€ ä, ä, 1ä, 3ät...éf'' ä s ä ®ä, »ä, af¥af^af†ä, f

af†ä, 1af^ä «ä, ^ä f ä | ç™°è | ä •ä, Cä ¾ä —ä Yä€,

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-info-exp-YXAWYP3s>

æ''è, å±Yæ'

af äf¼ä, äfSäf³	èª-æŽ	ä, »ä, -ä, afšäf³	ä, 1af†af¼ä, çä, 1	æ—Yä~
1.0	å^ å>žä...-é- <ä f ä f ä f¼ä, 1	-	Final	2022 å¹´ 4 æœ^ 6 æ—Y

å^©ç'''è! ç´,,

æœ-ä, çäf%ä f ä, ä, ¶ä, ¶ä f ä ç, ; ä ç è è ¼ä ®ä, ä ®ä " ä —ä | ä "æ ä ä¾>ä —ä | ä Šä, Šä€

æœ-ä, çäf%ä f ä, ä, ¶ä, ¶ä f ä ®æf...å ±ä Šä, ^ä ³ä f ä f ä, -ä ®ä½ç''' ä «é-çä™ä, <è²-ä»»ä ®ä, €

ä¾ä Yä€ ä, ä, 1ä, 3ä -æœ-ä f%ä, af¥af†ä f ä ®ät...å®¹ä, 'ä^å'Sä ä —ä «å%æ'ä —ä

æœ-ä, çäf%ä f ä, ä, ¶ä, ¶ä f ä ®è ~ è ç °ät...å®¹ä «é-çä —ä | æf...å ±è... ä ç j ä ® URL

ä, çœ ç ¥ä —ä ä ç <-ä ®è»ç è¼%ä,,, æ,, è ³ä, 'æ-½ä —ä Yä 'ä ^ä€ ä½"ç¾¾ä Cç®;ç

ä "ä ®ä f%ä, af¥af†ä f ä ®æf...å ±ä -ä€ ä, ä, 1ä, 3è£½ä" ä ®ä, "ä f ä f%ä f¼ä, ¶ä, 'ä¾±;

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。