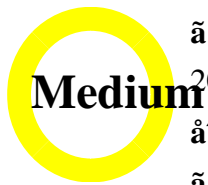


Cisco Unified Contact Center

Enterprise WebF™ 1.0, 1.0.1, 1.0.2, 1.0.3



Cisco Unified Contact Center Enterprise (UCCE) WebF ID : cisco-sa-20160622-ucce

[CVE-2016-1439](#)

Published : 2016-06-22 13:30

WebF 1.0 : Final

CVSS : 4.3

Workarounds : No workarounds available

Cisco Bug ID : [CSCux59474](#) [CSCux59650](#)

Summary Cisco Unified Contact Center Enterprise (UCCE) WebF 1.0, 1.0.1, 1.0.2, 1.0.3 is vulnerable to a Denial of Service (DoS) attack via a specially crafted HTTP request.

Details

Cisco Unified Contact Center Enterprise (UCCE) WebF 1.0, 1.0.1, 1.0.2, 1.0.3 is vulnerable to a Denial of Service (DoS) attack via a specially crafted HTTP request.

The vulnerability exists because the application fails to properly validate the length of the request body. An attacker can send a request with a large body, causing the application to consume excessive memory and crash.

The impact of this vulnerability is that an attacker can cause the application to crash, resulting in a Denial of Service (DoS) attack.

The severity of this vulnerability is Medium (CVSS 4.3).

There are no workarounds available for this vulnerability.

For more information, please refer to the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160622-ucce>

References

[CVE-2016-1439](#)

Cisco Unified Contact Center Enterprise (UCCE)

WebF 1.0, 1.0.1, 1.0.2, 1.0.3 is vulnerable to a Denial of Service (DoS) attack via a specially crafted HTTP request.

For more information, please refer to the following link:

[https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160622-ucce](#)

Ā>žė Ćċ-

ā, āfā, ā, ā, āfāf—āfā, āfā, °(XSS)æ''æ'fā "ā€ā"ā, Ćā, %ā@è,, †ā¼±æ€Śā, 'æ, ¢' "ā™ā
[ā, āfā, ā, ā, āfāf—āfā, āfā, °\(XSS\)ā@è,,...ā" āf™ā, āfāf«ā«āā, ā!ā€ā, ā, ¢, ...Śā](#)

ā; @æċæ, ^ā Ćā, ½āf•āf^ā, | ā, Śā, Ć

ā, ā, ā, āā Śā ā€Cisco
 Bugsā @ā; @æċæ, ^ā Ćā, ½āf•āf^ā, | ā, Śā, Ćā «é-Ćā™ā, <æf...ā ±ā, 'æ Ćāā¾ā —ā | ā, ā¾ā
[Cisco Bug Search Tool](#)ā <ā, %ā, Ćā, ā, ā, āā Śā ā¾ā™ā€,

ā, ½āf•āf^ā, ā, śā, ¢ā @ā, Ćāffāf—ā, °āf-āf¼āf%ā, 'ææœè "Žā™ā, <ā 'ā ^ā ā€
<http://www.cisco.com/go/psirt> ā @ Cisco Security Advisories and Responses
 ā, Ćāf¼ā, «ā, āf-ā,, ā¾ĆĈšā @ā, Ćāf%āf ā, ā, āfā, ā, ¢...Śā —ā | ā€ā¾µā®ā, ā —ā 'ā, <ā
 ā, ½āfāf¼ā, āfšāfā, 'ĉĆèªā —ā | āāā ā•ā, ā€.

ā, ā Śā, Ćā @ā 'ā ^ā, ā€ā, Ćāffāf—ā, °āf-āf¼āf%ā™ā, <āfāf ā, ā, ā «āā ^ā āfāfĆā
 Technical Assistance
 Centeri¼^TACi¼%ā,, ā —āāāā "ā'ĉ', ā —ā | ā, ā, <āfāfāfāfāfšāfā, āf—āfāf ā, āfĆāf¼ā«

ā, æċā^Ĉ Ć'' ā<ā¾ā" ā...-ā¼Ĉ™ºèj

Cisco Product Security Incident Response
 Teami¼^PSIRTi¼%ā ā€æœ-ā, Ćāf%āf ā, ā, āfāā «è"~è¼%ā•ā, Ćā | ā, ā, è,, †ā¼±æ€Śā™ā

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160622-ucce>

æ''è,, ā±Yæ'

āfāf¼ā, āfšāf³	èª-æ~Ž	ā, »ā, ā, āfšāf³	ā, āfāf¼ā, ā, ā¹	æ—Yā»~
1.0	ā^ ā>žā...-é-āfāāfāf¼ā,¹	-	Final	2016ā¹'6æœ^22æ—Y

ā^ĈĆ''è! Ć',

æœ-ā, ¢āf%āf ā, ā, āfāā Ć,, āĆ Ćè"¼ā @ā,, ā @ā "ā —ā | ā"æ Ćā¾ā —ā | ā Śā, Śā€
 æœ-ā, Ćāf%āf ā, ā, āfāā @æf...ā ±ā Śā, ^ā¾āfāfāfā, ā @ā¼Ć" "ā «é-Ćā™ā, è²-ā»ā @ā, €
 ā¾āYā€ā, ā, ā, āā æœ-āf%ā, āfāfāfāfāf^ā @āt...ā®¹ā, ā^ā'Sāāā —ā «ā%āæ'ā —ā
 æœ-ā, ¢āf%āf ā, ā, āfāā @è"~è:āt...ā®¹ā «é-Ćā —ā | æf...ā ±é... ā; ā @ URL

ã, 'çœ ç•¥ã —ã€ å ~ç<-ã ®è»çè¼%ã,,æ,, è ``³ã,'æ-½ã —ã ÿå 'å ^ã€ å½"ç³¼ã Çç®;ç
ã "ã ®ãf%ãã,ãf¥ãf;ãf³ãf^ã ®æf...å ±ã ¯ã€ ã,ã,ã,ã,³è£½å" ã ®ã, "ãf³ãf%ããf!ãf¼ã,¶ã,ã³¼è±;ã

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。