

Cisco Unified Contact Center Express

CCX Configurable SaaS, CVE-2014-2102 RCE



Severity: CVE-2014-2102
Product: Cisco Unified Contact Center Express (CCX) SaaS
Version: 10.0(1) and later
CVSS: 4.0
Workarounds: No Workarounds available
Cisco ID: CSCum95575

Summary: A remote code execution (RCE) vulnerability exists in the Cisco Unified Contact Center Express (CCX) SaaS. An attacker can exploit this vulnerability to execute arbitrary code on the affected system.

Impact

Cisco Unified Contact Center Express (Cisco Unified

CCX) SaaS, CVE-2014-2102 , RCE , CVSS: 4.0 , $\text{No Workarounds available}$, $\text{Cisco ID: CSCum95575}$

Details: The vulnerability is located in the `CCXConfigurableSaaS` component. It allows an attacker to execute arbitrary code on the affected system.

Exploit: The exploit is a remote code execution (RCE) attack. It involves sending a specially crafted request to the affected system, which then executes the arbitrary code.

Proof of Concept: A proof of concept (PoC) exploit is available for this vulnerability. It demonstrates how an attacker can execute arbitrary code on the affected system.

References: [Cisco Security Advisory: \$\text{CVE-2014-2102}\$](#) , [Cisco Bug ID: CSCum95575](#)

Conclusion

This vulnerability is a remote code execution (RCE) attack. It allows an attacker to execute arbitrary code on the affected system.

Bug ID: [CSCum95575](#), CVSS: 4.0 , $\text{No Workarounds available}$, $\text{Cisco ID: CSCum95575}$

Severity: CVE-2014-2102 , RCE , CVSS: 4.0 , $\text{No Workarounds available}$, $\text{Cisco ID: CSCum95575}$

Product: Cisco Unified Contact Center Express (CCX) SaaS, CVE-2014-2102 , RCE , CVSS: 4.0 , $\text{No Workarounds available}$, $\text{Cisco ID: CSCum95575}$

Unified

CCXā@æ-°ā—ā,,āfāāfāf¼ā,1ā«ā,,è,,†ā¼±æ€SāCEā~āce™ā,ā`èf¼æ€SāCEā,ā,Sā
è,,†ā¼±æ€Sā,ā«ā,āSā,,āā,ā"ā"āCEçç`èā•ā,CEāYèf¼ā"
ā»ā@ā,ā,1ā,³èf¼ā"ā«āSā,,ā|ā"ā@ā,čāf%āfā,ā,ā,āfā@ā½±éY;ā,ā—ā,ā,

ā>žéç-

ā»Sā¼CEā@ā,čāffāf—āf†āf¼āf^ā,,āfāāfāf¼ā,1ā«āā,,ā|ā-ā€āf™āf³āf€āf¼ā«é€çµjā

ä;é¼āSāā,čāf|āf¼ā,āāā'ā«āfāffāf^āfāf¼ā,ā,čā,ā,»ā,1ā,'è±ā-ā™ā,ā"ā"ā,ā,

ā½±éY;ā,ā—ā'ā,ā,ā,1āf†āfā,ç;£è|_ā™ā,ā"ā"ā,æŽ"ā¥"ā—ā¼ā™ā€,

ä;@æfæ,^āçã,½āf•āf^ā,|ā,Sā,ç

ā,½āf•āf^ā,|ā,šā,čā@æ'æ-°āf—āfā,°āf@āfā-ā^ç""āSāāā¼ā>ā,"ā€,

ä,æfā^ç""ä°<ā¼<ā"ā...-ā¼ç™°è;"

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%ā-ā€æœ-ā,čāf%āfā,ā,ā,āfā«è~¼%ā•ā,CEā|ā,,ā,è,,†ā¼±æ€Sā

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/Cisco-SA-20140227-CVE-2014-2102>

æ"¹è",ā±¥æ'

āfāf¼ā,,āfSāf³	è-æŽ	ā,»ā,ā,āfšāf³	ā,1āf†āf¼ā,ä,1	æ—¥ä»~
1.0	ā^ç%°^āfāāfāf¼ā,1	éçç""ā-	Final	2014ā¹2æœ^27æ-¥

ā^çç""è!ç,,

æœ-ā,čāf%āfā,ā,ā,āfā-ç,,jäçè"¼ā@ā,,ā@ā-ā-ā|ā"æçç¼ā-ā|āŠā,Šā€
æœ-ā,čāf%āfā,ā,ā,āfā@æf...ā±āŠā,^ā³āfāāfā,ā@ā½çç""ā«é-čā™ā,è²-ā»ā@ā,€
ā¼āYā€ā,ā,1ā,³āæœ-āf%ā,āfāfjāf³āfā@ā†...ā@¹ā,ā^ā'Sāāā-ā«ā%œ'ā-ā
æœ-ā,čāf%āfā,ā,ā,āfā@è~èç°ā†...ā@¹ā«é-čā-ā|æf...ā±é...äjä@ 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。