

Cisco Ultra Services Framework AutoVNF Symbolic Link Handling Information Disclosure Vulnerability



CVE ID : cisco-sa-20170705-usf1

[CVE-2017-6708](#)

Reported : 2017-07-05 16:00

Product : Final

CVSS : [7.5](#)

Workarounds : No workarounds available

Cisco ID : [CSCvc76654](#)

Symbolic link handling information disclosure vulnerability in Cisco Ultra Services Framework AutoVNF

Summary

Cisco Ultra Services Framework AutoVNF uses symbolic links to access files. A vulnerability was discovered in the handling of symbolic links that can result in information disclosure.

Impact – An attacker can access files that are not intended to be accessible. The severity of this vulnerability is High (CVSS 7.5).

Resolution – Cisco has released a patch to address this vulnerability in Cisco Ultra Services Framework AutoVNF 5.0.3.

References – Cisco Security Advisory [CSCvc76654](#)

For more information on this vulnerability, please see the [Cisco Security Advisory](#) at [https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf1](#).

Additional information on this vulnerability can be found in the [Cisco Security Advisory](#) at [https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf1](#).

Technical Details

The vulnerability is related to the handling of symbolic links in the `auto_vnf` module.

The affected versions are Cisco Ultra Services Framework AutoVNF 5.0.3.

The vulnerability is located in the `auto_vnf` module.

The vulnerability is caused by a flaw in the way symbolic links are processed. An attacker can use this vulnerability to access files that are not intended to be accessible.

ä;®æfæ,^ã;ãfãfãfãfã,¹

ã"ã®è,,†å¼±æ€§ã-ã€Cisco Ultra Services Framework ãfãfãfã,¹ 5.0.3 ãŠã,^ã³
5.1 ãSä;®æfã•ã,CEã¾ã—ãYã€,

ä,æfã^©ç"" ä°<ã¾ã"ã...-ã¼ç™ºè;''

Cisco Product Security Incident Response

Teami¼^PSIRTi¼%ã-ã€æœ-ã,Çãf%ããfã,ãã,¶ã,¶ãfãã«è~è¼%ã•ã,CEã|ã,,ã,<è,,†å¼±æ€§ã

ã†°ã...,

æœ-è,,†å¼±æ€§ã-ã€ã,ã,ã,¹ã,³ã†...éf"ãSã®ã,»ã,ãfãfãfãfã,£
ãfã,¹ãf^ã«ã,^ã£ã|ç™ºè|<ã•ã,CEã¾ã—ãYã€,

URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170705-usf1>

æ''è'',ã±Yæ'

ãfãfã,ãfãf³	èª-æ~Z	ã,»ã,ã,ãfãf³	ã,¹ãf†ãf¼ã,¿ã,¹	æ—Yã»~
1.0	ã^ã>ãžã...-é-ãfãfãfãfã,¹	-	Final	2017 å¹ 7 æœ^ 5 æ—Y

ã^©ç""è!ç',,,

æœ-ã,çãf%ããfã,ãã,¶ã,¶ãfãã-ç,,jãçè"¼ã®ã,,ã®ã"ã—ã|ã"æãã¾ãã—ã|ãŠã,Šã€
æœ-ã,Çãf%ããfã,ãã,¶ã,¶ãfãã®æf...ã±ãŠã,^ã³ãfãfãfã,ã®ã½çç""ã«é-Çã™ã,<è²-ã»ã®ã,€
ã¾ãYã€ã,ã,¹ã,³ã-æœ-ãf%ã,ãfãfãfãfãfã®ã†...ã®¹ã,'ã°ã'Sããã—ã«ã%ãæ'ã—ã
æœ-ã,çãf%ããfã,ãã,¶ã,¶ãfãã®è"~èç°ã†...ã®¹ã«é-Çã—ã|æf...ã±é...ãçjã® URL
ã,çœçç•ã—ã€ããçç-ã®è»Çè¼%ã,,,æ,,è"³ã,'æ-½ã—ãYã'ã^ã€ã½"ç¾ã¾CEç®;ç
ã"ã®ãf%ã,ãfãfãfãfãfã®æf...ã±ã-ã€ã,ã,¹ã,³è£½ã"ã®ã,"ãfãf%ããfãfã,¶ã,ã¾è±;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。