

# Cisco セキュア ブート ハードウェアの改ざんの脆弱性



アドバイザーID : cisco-sa-20190513-secureboot [CVE-2019-1649](#)

初公開日 : 2019-05-13 17:30

最終更新日 : 2019-11-20 17:23

バージョン 1.17 : Final

CVSSスコア : [6.7](#)

回避策 : No workarounds available

Cisco バグ ID : [CSCvn77158](#) [CSCvn77159](#)

[CSCvn77153](#) [CSCvn77154](#) [CSCvn77155](#)

[CSCvn77156](#) [CSCvn77150](#) [CSCvn77151](#)

[CSCvn77152](#) [CSCvn89138](#) [CSCvn89137](#)

[CSCvn77205](#) [CSCvn77249](#) [CSCvn77207](#)

[CSCvn77168](#) [CSCvn77201](#) [CSCvn77245](#)

[CSCvn77169](#) [CSCvn77202](#) [CSCvn77246](#)

[CSCvn77248](#) [CSCvn77166](#) [CSCvn77167](#)

[CSCvn77160](#) [CSCvp42792](#) [CSCvn77162](#)

[CSCvn77170](#) [CSCvn89140](#) [CSCvn77209](#)

[CSCvn89146](#) [CSCvn89145](#) [CSCvn89144](#)

[CSCvn89143](#) [CSCvn77219](#) [CSCvn77212](#)

[CSCvn77175](#) [CSCvn77171](#) [CSCvn77172](#)

[CSCvn77180](#) [CSCvn77181](#) [CSCvn89150](#)

[CSCvn77147](#) [CSCvn77142](#) [CSCvn77143](#)

[CSCvn77220](#) [CSCvn77182](#) [CSCvn77183](#)

[CSCvn77184](#) [CSCvn77141](#) [CSCvn77185](#)

[CSCvn77191](#)

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

## 概要

シスコ独自のセキュア ブート実装に含まれるハードウェア コンポーネントの 1 つに対するアクセス制御を処理するロジックの脆弱性により、認証されたローカルの攻撃者が該当コンポーネントに改ざんしたファームウェア イメージを書き込める危険性があります。この脆弱性はハードウェア ベースのセキュア ブートをサポートする複数のシスコ製品に影響を及ぼします。

この脆弱性は、セキュア ブート ハードウェア実装の Field Programmable Gate Array ( FPGA ) 部分に対するオンプレミス アップデートを管理するコードの領域が適切にチェックされないことに起因します。昇格された特権を持ち、該当デバイスで動作する基盤となるオペレーティングシステムにアクセスできる攻撃者が、FPGA に改ざんされたファームウェア イメージを書き込むことにより、この脆弱性をエクスプロイトする危険性があります。エクスプロイトが成功すると、デバイスが使用不能になる ( ハードウェアの交換が必要になる ) かセキュア ブート検証プロセスでの改ざんが可能になり、攻撃者が悪意のあるソフトウェア イメージインストールして起動する恐れがあります。

シスコでは、この脆弱性に対処するソフトウェア アップデートをリリースする予定です。この脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot>

## 該当製品

### 脆弱性のある製品

次の表に、本アドバイザリに記載された脆弱性の影響を受けるシスコ製品を示します。

この表には、影響を受ける各製品の Cisco Bug ID が記載されています。バグは [Cisco バグ検索ツール](#)で検索できるようになっており、それぞれにプラットフォームに固有の追加情報と修正済みリリースが記載されます。

将来のソフトウェア リリース日が示されている場合、その日付はこのアドバイザリの上部にある最終更新日時時点でシスコが把握しているすべての情報に基づいた日付になります。このソフトウェア リリースの日付は、試験結果や優先される機能や修正の提供等いくつかの理由により変更される場合があります。影響を受けるコンポーネントについてバージョン情報や日付がリストに記載されていない場合 ( 空欄や暫定とされているもの )、シスコは修正の評価を続けており、追加情報が確認された時点でアドバイザリを更新します。アドバイザリが Final とマークされた後、より詳細な情報については関連する Cisco バグを参照して下さい。

製品	Cisco Bug ID	Fixed Release Availability
ネットワークおよびコンテンツ セキュリティ デバイス		
Cisco ASA 5506-X	<a href="#">CSCvn77246</a>	ファームウェアリリース1.1.15 ( イメージ名 : asa5500-firmware-1115.SPA ) ( 入手可能 )
Cisco ASA 5506H-X	<a href="#">CSCvn77246</a>	ファームウェアリリース1.1.15 ( イメージ名 : asa5500-firmware-1115.SPA ) ( 入手可能 )
Cisco ASA 5506W-X	<a href="#">CSCvn77246</a>	ファームウェアリリース1.1.15 ( イメージ名 : asa5500-firmware-1115.SPA ) ( 入手可能 )

Cisco ASA 5508-X	<a href="#">CSCvn77246</a>	ファームウェアリリース1.1.15 ( イメージ名 : asa5500-firmware-1115.SPA ) ( 入手可能 )
Cisco ASA 5516-X	<a href="#">CSCvn77246</a>	ファームウェアリリース1.1.15 ( イメージ名 : asa5500-firmware-1115.SPA ) ( 入手可能 )
Cisco Firepower 2100 シリーズ	<a href="#">CSCvn77248</a>	<p>Cisco Firepower Threat Defense ( FTD ) ソフトウェア 6.2.2.5 ホットフィックス ( 入手可能 )</p> <p>Cisco Firepower Threat Defense ( FTD ) ソフトウェア 6.2.3.12 ホットフィックス ( 入手可能 )</p> <p>Cisco Firepower Threat Defense ( FTD ) ソフトウェア 6.3.0.3 ホットフィックス ( 入手可能 )</p> <p>Cisco Firepower Threat Defense ( FTD ) ソフトウェア 6.2.3.13 ( 入手可能 )</p> <p>Cisco Firepower Threat Defense ( FTD ) ソフトウェア 6.4.0.1 ( 入手可能 )</p> <p>Cisco 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア 9.8.4.3 ( 入手可能 )</p> <p>Cisco 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア 9.9.2.50 ( 入手可能 )</p> <p>Cisco 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア 9.9.2.52 ( 入手可能 )</p> <p>Cisco 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア 9.10.1.22 ( 入手可能 )</p> <p>Cisco 適応型セキュリティ アプライアンス ( ASA ) ソフトウェア 9.12.2 ( 入手可能 )</p>
Cisco Firepower 4000 シリーズ	<a href="#">CSCvn77249</a>	ファームウェアバンドルパッケージv1.0.18、ROMMON rev 1.0.15およびFPGA rev 2.0: ( イメージ名 : fxos-k9-fpr4k-firmware.1.0.18.SPAおよびfxos-k9-fpr9k-firmware.1.0.18.SPA ) ( 入手可能 )
Cisco Firepower 9000 シリーズ	<a href="#">CSCvn77249</a>	ファームウェアバンドルパッケージv1.0.18、ROMMON rev 1.0.15およびFPGA rev 2.0: ( イメージ名 : fxos-k9-fpr4k-firmware.1.0.18.SPAおよびfxos-k9-fpr9k-firmware.1.0.18.SPA ) ( 入手可能 )
Routing and Switching - Enterprise and Service Provider		
10/40/100G MR マックス ポンド : 暗号化用使用権 ライセンス ( NCS2K-MR- MXP-LIC )	<a href="#">CSCvn77191</a>	11.1 ( 2019 年 7 月 )
Cisco NCS 2000 シリー ズおよび Cisco ONS 15454 MSTP 用 10 Gbps	<a href="#">CSCvn77191</a>	11.1 ( 2019 年 7 月 )

光暗号化ラインカード ( 15454-M-WSE-K9 )		
ASR 903 ルータ、スイッチングプロセッサおよびコントローラ - 400G ( A900-RSP3C-400-S )	<a href="#">CSCvn77169</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
ASR 907 ルータ、スイッチングプロセッサおよびコントローラ - 400G ( A900-RSP3C-400-W )	<a href="#">CSCvn77169</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
CBR-8 コンバインドブロードバンドルータ	<a href="#">CSCvn77185</a>	Cisco IOS XE ソフトウェアリリース 16.12.1w ( 2019 年 9 月 )
Catalyst 6800 16 ポート 10GE、統合型 DFC4 ( C6800-16P10G )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Catalyst 6800 32 ポート 10GE、統合型デュアル DFC4 ( C6800-32P10G )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Catalyst 6800 8 ポート 10GE、統合型 DFC4 ( C6800-8P10G )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6800 ( 40 GE ポート X 8、統合型デュアル DFC4-EXL X 2 ) ( C6800-8P40G-XL )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco 1 ポート ギガビットイーサネット WAN ネットワーク インターフェイス モジュール ( NIM-1GE-CU-SFP )	<a href="#">CSCvn77218</a>	Cisco IOS XE ソフトウェア リリース 16.9.5 ( 1 月 20 日 ) Cisco IOS XE ソフトウェア リリース 16.12.2 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 17.1.1 ( 2019 年 11 月 )
Cisco 1120 Connected Grid ルータ	<a href="#">CSCvn89140</a>	Cisco IOS ソフトウェア リリース 15.9(3)M ( 2019 年 8 月 ) Cisco IOS ソフトウェア リリース 15.8(3)M3 ( 2019 年 8 月 ) Cisco IOS ソフトウェア リリース 15.7(3)M5 ( 2019 年 9 月 ) Cisco IOS ソフトウェア リリース

		15.6(3)M7 ( 2019 年 9 月 )
Cisco 1240 Connected Grid ルータ	<a href="#">CSCvn89137</a>	Cisco IOS ソフトウェア リリース 15.9(3)M ( 2019 年 8 月 ) Cisco IOS ソフトウェア リリース 15.8(3)M3 ( 2019 年 8 月 ) Cisco IOS ソフトウェア リリース 15.7(3)M5 ( 2019 年 9 月 ) Cisco IOS ソフトウェア リリース 15.6(3)M7 ( 2019 年 9 月 )
Cisco 2 ポート ギガビットイーサネット WAN ネットワーク インターフェイス モジュール ( NIM-2GE-CU-SFP )	<a href="#">CSCvn77218</a>	Cisco IOS XE ソフトウェア リリース 16.9.5 ( 1 月 20 日 ) Cisco IOS XE ソフトウェア リリース 16.12.2 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 17.1.1 ( 2019 年 11 月 )
Cisco 3000 シリーズ産業用セキュリティ アプライアンス	<a href="#">CSCvn89146</a>	ファームウェアリリース1.0.05 ( イメージ名 : isa3000-firmware-1005.SPA ) ( 入手可能 )
Cisco 4000 シリーズ サービス統合型ルータ パケット 1024 チャンネル高密度音声 DSP モジュール ( SM-X-PVDM-1000 )	<a href="#">CSCvn77212</a>	Cisco IOS XE ソフトウェア リリース 16.12.2 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 17.1.1 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 16.9.5 ( 1 月 20 日 )
Cisco 4000 シリーズ サービス統合型ルータ パケット 2048 チャンネル高密度音声 DSP モジュール ( SM-X-PVDM-2000 )	<a href="#">CSCvn77212</a>	Cisco IOS XE ソフトウェア リリース 16.12.2 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 17.1.1 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 16.9.5 ( 1 月 20 日 )
Cisco 4000 シリーズ サービス統合型ルータ パケット 3080 チャンネル高密度音声 DSP モジュール ( SM-X-PVDM-3000 )	<a href="#">CSCvn77212</a>	Cisco IOS XE ソフトウェア リリース 16.12.2 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 17.1.1 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 16.9.5 ( 1 月 20 日 )
Cisco 4000 シリーズ サービス統合型ルータ パケット 768 チャンネル高密度音声 DSP モジュール ( SM-	<a href="#">CSCvn77212</a>	Cisco IOS XE ソフトウェア リリース 16.12.2 ( 2019 年 11 月 ) Cisco IOS XE ソフトウェア リリース 17.1.1 ( 2019 年 11 月 )

X-PVDM-500 )		Cisco IOS XE ソフトウェア リリース 16.9.5 ( 1 月 20 日 )
Cisco 4221 サービス統合型ルータ	<a href="#">CSCvn77153</a>	ユーティリティファイル名 : isr4200_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 4321 サービス統合型ルータ	<a href="#">CSCvn77156</a>	ユーティリティファイル名 : isr4300_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 4331 サービス統合型ルータ	<a href="#">CSCvn77156</a>	ユーティリティファイル名 : isr4300_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 4351 サービス統合型ルータ	<a href="#">CSCvn77156</a>	ユーティリティファイル名 : isr4300_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 4431 サービス統合型ルータ	<a href="#">CSCvn77155</a>	ユーティリティファイル名 : isr4400_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 4451-X サービス統合型ルータ	<a href="#">CSCvn77155</a>	ユーティリティファイル名 : isr4400_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 4461 サービス統合型ルータ	<a href="#">CSCvn77154</a>	ユーティリティファイル名 : isr4400v2_cpld_update_v1.1_SPA.bin ( 入手可能 )
Cisco 5000 シリーズ エンタープライズ ネットワーク コンピュータ システム	<a href="#">CSCvn77150</a>	リリース番号未定 ( 2019 年 8 月 )
Cisco 809 Industrial サービス統合型ルータ	<a href="#">CSCvn89138</a>	Cisco IOS ソフトウェア リリース 15.8(3)M2a ( 入手可能 ) Cisco IOS ソフトウェア リリース 15.7(3)M4b ( 入手可能 ) Cisco IOS ソフトウェア リリース 15.6(3)M6b ( 入手可能 )
Cisco 829 産業用サービス統合型ルータ	<a href="#">CSCvn89143</a>	Cisco IOS ソフトウェア リリース 15.8(3)M2a ( 入手可能 ) Cisco IOS ソフトウェア リリース 15.7(3)M4b ( 入手可能 ) Cisco IOS ソフトウェア リリース 15.6(3)M6b ( 入手可能 )
Cisco ASR 1000 インベ	<a href="#">CSCvn77159</a>	リリース番号未定 ( 2019 年 12 月 )

デッド サービス プロセッサ 200G ( ASR1000-ESP200 )		
Cisco ASR 1000 固定型イーサネット ライン カード ( 10 GE X 6 ) ( ASR1000-6TGE )	<a href="#">CSCvn89144</a>	リリース番号未定 ( 2019 年 12月 )
Cisco ASR 1000 固定型イーサネット ライン カード ( 10 GE X 2 + 1 GE X 20 ) ( ASR1000-2T+20X1GE )	<a href="#">CSCvn89144</a>	リリース番号未定 ( 2019 年 12月 )
Cisco ASR 1000 シリーズ 100 Gbps エンベデッド サービス プロセッサ ( ASR1000-ESP100 )	<a href="#">CSCvn77160</a>	リリース番号未定 ( 2019 年 12月 )
Cisco ASR 1000 シリーズ モジュラ インターフェイス プロセッサ ( ASR1000-MIP100 )	<a href="#">CSCvn77158</a>	リリース番号未定 ( 2019 年 12月 )
Cisco ASR 1000 シリーズ ルート プロセッサ 3 ( Cisco ASR1000-RP3 )	<a href="#">CSCvn77167</a>	リリース番号未定 ( 2019 年 12月 )
Cisco ASR 1001-HX ルータ	<a href="#">CSCvn77162</a>	ASR1K-fpga_prog.16.0.0.xe.bin ( 入手可能 )
Cisco ASR 1001-X	<a href="#">CSCvn89145</a>	ASR1K-fpga_prog.16.0.0.xe.bin ( 入手可能 )
Cisco ASR 1002-HX ルータ	<a href="#">CSCvn77166</a>	ASR1K-fpga_prog.16.0.0.xe.bin ( 入手可能 )
Cisco ASR 900 シリーズ ルート スイッチ プロセッサ ( 2 ~ 128 G、基本スケール ) ( A900-RSP2A-128 )	<a href="#">CSCvn77168</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 900 シリーズ ルート スイッチ プロセッサ ( 2 ~ 64 G、基本スケール ) ( A900-RSP2A-64 )	<a href="#">CSCvn77168</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )

Cisco ASR 900 シリーズ ルートスイッチプロセッサ ( 3 ~ 200 G、大規模スケール ) ( A900-RSP3C-200 )	<a href="#">CSCvn77169</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 9000 シリーズ 16 ポート 100 ギガビットイーサネットラインカード ( A99-16X100GE-X-SE )	<a href="#">CSCvn77180</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR 9000 シリーズ 16 ポート 100 ギガビットイーサネットラインカード ( A9K-16X100GE-TR、A9K-16X100GE-CM )	<a href="#">CSCvn77180</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR 9000 シリーズ 32 ポート 100 ギガビットイーサネットラインカード ( A99-32X100GE-TR、A99-32X100GE-CM )	<a href="#">CSCvn77180</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR 9000 シリーズ ルートスイッチプロセッサ 5 ( パケット転送用 ) ( A9K-RSP5-TR )	<a href="#">CSCvn77175</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR 9000 シリーズ ルートスイッチプロセッサ 5 ( サービスエッジ用 ) ( A9K-RSP5-SE )	<a href="#">CSCvn77175</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーションサービスルータ 10GE および 2 ~ 10GE - パッシブ冷却 DC モデル ( ASR-920-10SZ-PD )、Cisco ASR920 シリーズ - 20GE SFP、4Cu および 4 ~ 10GE : モジュラ PSU ( ASR-920-20SZ-M )	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )

Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 1/10 GE SFP X 12、AC モデル ) ( ASR-920-12SZ-A )	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 1/10 GE SFP X 12、DC モデル ) ( ASR-920-12SZ-D )	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 12 GE および 2 ~ 10 GE、AC モデル ) ( ASR-920-12CZ-A )	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 12 GE および 2 ~ 10 GE、DC モデル ) ( ASR-920-12CZ-D )	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 24 GE 銅線お よび 4 ~ 10 GE、モジュ ラ PSU ) ( ASR-920-24TZ- M )	<a href="#">CSCvn77172</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ 24GE ファイバお よび 4-10GE - モジュ ラ PSU ( ASR-920-24SZ-M )	<a href="#">CSCvn77172</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 2 GE および 4 ~ 10 GE、AC モデル ) ( ASR-920-4SZ-A )	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( 2 GE および 4 ~ 10 GE、DC モデル	<a href="#">CSCvn77171</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )

) ( ASR-920-4SZ-D )		
Cisco ASR 920 シリーズ アグリゲーション サービス ルータ ( コンフォーマ ル コーティング、12 GE および 4 ~ 10 GE、1 IM スロット ) ( ASR-920- 12SZ-IM-CC )	<a href="#">CSCvn77170</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR 9900 ルート プロセッサ 3 ( パケット 転送用 ) ( A99-RP3- TR )	<a href="#">CSCvn77175</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR 9900 ルート プロセッサ 3 ( サービス エッジ用 ) ( A99-RP3- SE )	<a href="#">CSCvn77175</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco ASR920 シリーズ - 12GE および 4-10GE、1 IM スロット ( ASR-920- 12SZ-IM )	<a href="#">CSCvn77170</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco ASR920 シリーズ - 24GE および 4-10GE - モ ジュラ PSU および IM ( ASR-920-24SZ-IM )	<a href="#">CSCvn77172</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco Catalyst 6800 ( 16 ポート 10 GE、統合型 DFC4-XL ) ( C6800- 16P10G-XL )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6800 ( 32 ポート 10 GE、統合型デ ュアル DFC4-XL X 2 ) ( C6800-32P10G- XL )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6800 ( 8 ポート 10 GE、統合型 DFC4-XL ) ( C6800- 8P10G-XL )	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6800 ( 8 ポート 40 GE、統合型デ ュアル DFC4-EXL X	<a href="#">CSCvn77182</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )

2) ( C6800-8P40G-XL )		
Cisco Catalyst 6800 シリーズ スーパーバイザ エンジン 6T ( C6800-SUP6T )	<a href="#">CSCvn77181</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6800 シリーズ スーパーバイザ エンジン 6T XL ( C6800-SUP6T-XL )	<a href="#">CSCvn77181</a>	Cisco IOS XE ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6816-X-シャーシ ( 標準テーブル ) ( C6816-X-LE )	<a href="#">CSCvn77183</a>	Cisco IOS ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6824-X シャーシおよび 40 G X 2 ( 標準テーブル ) ( C6824-X-LE-40G )	<a href="#">CSCvn77183</a>	Cisco IOS ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6832-X シャーシ ( 標準テーブル ) ( C6832-X-LE )	<a href="#">CSCvn77183</a>	Cisco IOS ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 6840-X シャーシおよび 40G x 2 ( 標準テーブル ) ( C6840-X-LE-40G )	<a href="#">CSCvn77183</a>	Cisco IOS ソフトウェア リリース 15.5(1)SY4 ( 2019 年 9 月 )
Cisco Catalyst 9300 シリーズ スイッチ	<a href="#">CSCvn77209</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpgutility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズ高性能スイッチ ( 1/10/25 G ギガビットイーサネット X 24 + 40/100 G アップリンク X 4 ) ( C9500-24Y4C )	<a href="#">CSCvn89150</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpgutility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズ高性能スイッチ ( 100 ギガビットイーサネット X 32 ) ( C9500-32C )	<a href="#">CSCvn89150</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpgutility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズ高性能スイッチ ( 40 ギガビットイーサネット	<a href="#">CSCvn89150</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpgutility.SPA.bin ( 入手可能 )

X 32 ) ( C9500-32QC )		
Cisco Catalyst 9500 シリーズ高性能スイッチ ( 1/10/25 G ギガビットイーサネット X 48 + 40/100 G アップリンク X 4 ) ( C9500-48Y4C )	<a href="#">CSCvn89150</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpggautility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズスイッチ ( 40 G ギガビットイーサネット X 12 ) ( C9500-12Q )	<a href="#">CSCvn77220</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpggautility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズスイッチ ( 1/10 G ギガビットイーサネット X 16 ) ( C9500-16X )	<a href="#">CSCvn77220</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpggautility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズスイッチ ( 40 G ギガビットイーサネット X 24 ) ( C9500-24Q )	<a href="#">CSCvn77220</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpggautility.SPA.bin ( 入手可能 )
Cisco Catalyst 9500 シリーズスイッチ ( 1/10 G ギガビットイーサネット X 40 ) ( C9500-40X )	<a href="#">CSCvn77220</a>	ユーティリティ名 : cat9k_iosxe.16.00.00fpggautility.SPA.bin ( 入手可能 )
Cisco Catalyst 9600 スーパーバイザ エンジン 1	<a href="#">CSCvn95346</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 ( 2019 年 7 月 )
Cisco Catalyst 9800-40 ワイヤレス コントローラ	<a href="#">CSCvn77165</a>	C9800-40_fpga_prog.16.0.0.xe.bin ( 入手可能 )
Cisco Catalyst 9800-80 ワイヤレス コントローラ	<a href="#">CSCvn77163</a>	C9800-80_fpga_prog.16.0.0.xe.bin ( 入手可能 )
Cisco IC3000 産業用コンピューティング ゲートウェイ	<a href="#">CSCvp42792</a>	ファームウェア リリース 1.0.2 ( イメージ名 IC3000-K9-1.0.3.SPA ) ( 2019 年 8 月 )
Cisco MDS 9000 ファミリー 24/10 SAN 拡張モジュール ( DS-X9334-K9 )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco NCS 200 シリーズ	<a href="#">CSCvn77191</a>	11.1 ( 2019 年 7 月 )

10/40/100 G MR マックスポンダ ( NCS2K-MR-MXP-K9 )		
Cisco NCS 5500 12X10、2X40 2XMPA ラインカードベース ( NC55-MOD-A-S )	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 5500 シリーズ 24 ポート 100 GE および 12 ポート 40 GE ハイスケール ラインカード ( NC55-24H12F-SE )	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 5500 シリーズ 36 ポート 100 GE ハイスケール ラインカード ( NC55-36X100G-A-SE )	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 5504 ファブリックカード ( NC55-5504-FC )	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 5516 ファブリックカード ( NC55-5516-FC )	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA シャーシ ( NCS-55A2-MOD-S )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA シャーシ ( 温度耐性強化 ) ( NCS-55A2-MOD-HD-S )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA シャーシ ( 温度耐性強化、コンフォーマルコーティング ) ( NCS-55A2-MOD-HX-S )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )

スケールシャーシ ( NCS-55A2-MOD-SE-S )		
Cisco NCS 55A2 固定 10 G X 24 + 25 G X 16 MPA スケールシャーシ ( コンフォーマルコーティングによる温度耐性強化 ) ( NC55A2-MOD-SE-H-S )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS5501 10G X 40 および 100 G X 4 スケールシャーシ ( NCS-5501-SE )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS5501 固定 10G X 48 および 100 G X 6 シャーシ ( NCS-5501 )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS5502 100 G X 48 スケールシャーシ ( NCS-5502-SE )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS5502 固定 100 G X 48 シャーシ ( NCS-5502 )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS55A1 固定 100 G X 24 シャーシ ( NCS-55A1-24H )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS55A1 固定 100 G X 36 ベースシャーシ ( NCS-55A1-36H-S )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco NCS55A1 固定 100 G X 36 スケールシャーシ ( NCS-55A1-36H-SE-S )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco Network Convergence System 1001	<a href="#">CSCvvp88427</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )
Cisco Network Convergence System 1002	<a href="#">CSCvn77219</a>	Cisco IOS XR ソフトウェア リリース 7.0.1 ( 2019 年 7 月 )

Cisco Network Convergence System 5001	<a href="#">CSCvn77207</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco Network Convergence System 5002	<a href="#">CSCvn77205</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco ネットワーク コン バージェンスシステム 540 ( N540-ACC-SYS、 N540-24Z8Q2C-M、 N540-24Z8Q2C-SYS )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco ネットワーク コン バージェンス システム 540 コンフォーマル コー ディング ( N540X-ACC- SYS )	<a href="#">CSCvn77201</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco Network Convergence System 5500シリーズ : 1.2 Tbps IPoDWDMモジュラライ ンカード(NC55-6X200- DWDM-S)	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco Network Convergence System 5500シリーズ : 36X100G MACsecモジュラライン カード(NC55-36X100G- S)	<a href="#">CSCvn77202</a>	Cisco IOS XR ソフトウェア リリース 7.1.1 ( 2019 年 11 月 )
Cisco Nexus 31108PC- V ( SFP+ ポート X 48 お よび QSFP28 ポート X 6 ) ( N3K-C31108PC- V )	<a href="#">CSCvn77245</a>	Cisco NX-OS ソフトウェア リリース 9.3(1) ( 2019 年 8 月 )
Cisco Nexus 31108TC- V ( 10 G BASE-T RJ-45 ポート X 48 および QSFP28 ポート X 6 ) ( N3K-C31108TC- V )	<a href="#">CSCvn77245</a>	Cisco NX-OS ソフトウェア リリース 9.3(1) ( 2019 年 8 月 )
Cisco Nexus 3132C-Z ス	<a href="#">CSCvn77245</a>	Cisco NX-OS ソフトウェア リリース 9.3(1) ( 2019

スイッチ ( N3K-C3132C-Z )		年 8 月 )
Cisco Nexus 3264C-E スイッチ ( N3K-C3264C-E )	<a href="#">CSCvn77245</a>	Cisco NX-OS ソフトウェア リリース 9.3(1) ( 2019 年 8 月 )
Cisco Nexus 7000 M3 シリーズ 48 ポート 1/10 G イーサネット モジュール ( N7K-M348XP-25L )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco Nexus 7700 F4 シリーズ 30 ポート 100 G イーサネット モジュール ( N77-F430CQ-36 )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco Nexus 7700 M3 シリーズ 12 ポート 100 G イーサネット モジュール ( N77-M312CQ-26L )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco Nexus 7700 M3 シリーズ 24 ポート 40 G イーサネット モジュール ( N7K-M324FQ-25L )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco Nexus 7700 M3 シリーズ 48 ポート 1/10 G イーサネット モジュール ( N77-M348XP-23L )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco Nexus 7700 スーパーバイザ 3 ( N77-SUP3E )	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 ( 2019年9月 ) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-

		OSソフトウェアリリース8.4.1a ( 2019年9月 )
Cisco Nexus 9200 ( 40G 100G QSFP28 ポート X 36 ( N9K-C9236C ) )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9200 ( 1/10G/25G SFP+ ポート X 48 および 40G QSFP ポート X 6 または 100G QSFP28 ポート X 4 ( N9K-C92160YC-X )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9200 ( 10/25 Gbps ポート X 48、100G QSFP28 ポート X 18 ) ( N9K-C92300YC )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9200 ( 40G QSFP+ ポート X 56 および 100G QSFP28 ポート X 8 ( N9K-C92304QC )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9200 ( 40G QSFP+ ポート X 72 ) ( N9K-C9272Q )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9300 ( 1/10G/25G SFP ポート X 48、40G/100G QSFP28 ポート X 6、MACsec、ユニファイドポート対応 ) ( N9K-C93180YC-FX )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9300 ( 100M/1G BASE-T ポート X 48、10/25G SFP28 ポート X 4、40G/100G SFP28 ポート X 2 ) ( N9K-C9348GC-FXP )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI: スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9300 ( 10G BASE-T ポート X 48、	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 )

40G/100G QSFP28 ポート X 6、MACsec 対応 ) ( N9K-C93108TC-FX )		ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9332C スパインスイッチ ( 40/100G QSFP28 ポート X 32、1/10G SFP ポート X 2 ( N9K-C9332C ) )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9364C スパインスイッチ ( 40/100G QSFP28 ポート X 64、1/10G SFP ポート X 2 ( N9K-C9364C ) )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9500 4 コア /4 スレッド スーパーバイザ ( N9K-SUP-A )	<a href="#">CSCvn77142</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9500 6 コア /12 スレッド スーパーバイザ ( N9K-SUP-B )	<a href="#">CSCvn77142</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9000 固定、40G/100G QSFP28 ポート X 32 ( N9K-C9232C ) )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9000 固定、40G/100G QSFP28 ポート X 36 ( N9K-C9336C-FX2 )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9000 固定 ( 1/10G/25G SFP ポート X 48、40G/100G QSFP28 ポート X 12 ) ( N9K-C93240YC-FX2 )	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )
Cisco Nexus 9000 固定 ( 1/10G/25G SFP ポート X 48、40G/100G QSFP28 ポート X	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) ( 2019年8月 ) ACI : スイッチソフトウェアリリース 4.2(1) ( 2019年8月 )

6) (N9K-C93180YC-EX)		
Cisco Nexus 9000 固定 (10G BASE-T ポート X 48、40G/100G QSFP28 ポート X 6) (N9K-C93108TC-EX)	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) (2019年8月) ACI: スイッチソフトウェアリリース 4.2(1) (2019年8月)
Cisco Nexus 9000 固定 (40/50G QSFP+ ポート X 32 (最大) または 100G QSFP28 ポート X 18 (最大)) (N9K-C93180LC-EX)	<a href="#">CSCvn77143</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) (2019年8月) ACI: スイッチソフトウェアリリース 4.2(1) (2019年8月)
Cisco Packet-over-T3/E3 サービス モジュール (SM-X-1T3/E3)	<a href="#">CSCvn77147</a>	リリース番号未定 (2019年10月)
Cisco cBR-8 統合型 CCAP 40G リモート PHY ラインカード (CBR-CCAP-LC-40G-R)	<a href="#">CSCvn77184</a>	Cisco IOS XE ソフトウェア リリース 16.12.1 (2019年7月)
MDS 9700 48 ポート 32 Gbps ファイバチャネル スイッチング モジュール (DS-X9648-1536K9)	<a href="#">CSCvn77141</a>	N7K-M348XP-25L、N7K-M324FQ-25L、N77-M348XP-23L、N77-M31 2CQ-26L、N77-F430CQ-36、およびN77-M324FQ: Cisco NX-OSソフトウェアリリース8.4.2 (2019年9月) DS-X9648-1536K9およびDS-X9334-K9: Cisco NX-OSソフトウェアリリース8.4.1a (2019年9月)
Nexus 9500 用スーパーバイザ A+ (N9K-SUP-A+)	<a href="#">CSCvn77142</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) (2019年8月) ACI: スイッチソフトウェアリリース 4.2(1) (2019年8月)
Nexus 9500 用スーパーバイザ B+ (N9K-SUP-B+)	<a href="#">CSCvn77142</a>	NX-OS: Cisco NX-OSソフトウェアリリース 9.3(1) (2019年8月) ACI: スイッチソフトウェアリリース 4.2(1) (2019年8月)
<b>音声およびユニファイド コミュニケーション デバイス</b>		
Cisco 4000 シリーズ ISR 用アナログ音声ネットワーク インターフェイス モジュール (NIM-2FXO、NIM-4FXO、NIM-2FXS、	<a href="#">CSCvn77151</a>	リリース番号未定 (2019年9月)

NIM-4FXS、NIM-2FXS/4FXO、NIM-2FXSP、NIM-4FXSP、NIM-2FXS/4FXOP、NIM-4E/M、NIM-2BRI-NT/TE、NIM-4BRI-NT/TE )		
Cisco 4000 シリーズ サービス統合型ルータ T1/E1 音声および WAN ネットワーク インターフェイス モジュール ( NIM-1MFT-T1/E1、NIM-2MFT-T1/E1、NIM-4MFT-T1/E1、NIM-8MFT-T1/E1、NIM-1CE1T1-PRI、NIM-2CE1T1-PRI、NIM-8CE1T1-PRI )	<a href="#">CSCvn77152</a>	リリース番号未定 ( 2019 年 9 月 )

## 脆弱性を含んでいないことが確認された製品

シスコでは、ハードウェアベースのセキュア ブート機能をサポートするすべてのシスコ製品を調査し、適切なアクセス制御チェックが行われていることを確認済みです。

このアドバイザリの[脆弱性のある製品セクションに記載されている製品のみが、この脆弱性の影響を受けることが分かっています。](#)

ハードウェアベースのセキュア ブート機能をサポートするその他のシスコ製品には、脆弱性は存在しません。

## 詳細

攻撃者がこの脆弱性のエクスプロイトを試みるには、次の条件をすべて満たす必要があります。

- デバイスの特権管理アクセス権を持っている。
- デバイスで実行されている基盤となるオペレーティングシステムにアクセスできること。これは、サポートされている文書化されたメカニズムを使用するか、攻撃者にアクセスを提供する別の脆弱性を不正利用することで実現できます。
- プラットフォームに固有のエクスプロイトを作成したり、そのようなエクスプロイトにアクセスしたりできる。攻撃者が影響を受ける複数のプラットフォームでこの脆弱性のエクスプロイトを試みるには、それぞれのプラットフォームを調べてプラットフォームに固有のエクスプロイトを作成する必要があります。別のプラットフォームで調査プロセスを再利用でき

ることもありますが、特定のハードウェア プラットフォーム向けに作成されたエクスプロイトが別のハードウェア プラットフォームに影響を与えることはないと思われま

シスコでは、影響を受けるすべてのプラットフォームを対象としたソフトウェア修正プログラムの開発とリリースを進めています。ほとんどの場合、この脆弱性を修正するには、デバイスを正常に動作させるのに必要な下位レベルのハードウェア コンポーネントをオンプレミスで再プログラミングしなければなりません。このリプログラミング プロセスで障害が起きると、デバイスが使用不能になり、ハードウェアの交換が必要になることがあります。お客様におかれましては、お使いのプラットフォームに関連する Cisco Bug の Release Note Enclosure で次の情報を参照されることをお勧めします。

1. 再プログラミング プロセスでの障害につながり、デバイスが使用不能になる危険性がある原因
2. デバイスをリプログラミングするために必要なプラットフォーム固有の手順
3. 特定のデバイスで ( 修正が必要な ) 該当のファームウェア バージョンが実行されているのか、すでに修正済みのファームウェア バージョンが実行されているのかを確認するのに必要な手順

上記のリストの項目 2 と 3 の詳細は、各プラットフォームに固有の修正済みソフトウェア リリースとともに公開される製品のリリース ノートに記載される予定です。この製品のリリース ノートがこれらの項目に関する最新の情報源であるとお考えください。

セキュア ブートとそれに関連する Trustworthy テクノロジーの詳細については、[Trustworthy テクノロジーのデータシート](#)を参照してください。セキュアブートテクノロジーをサポートするすべてのシスコ製品のリストについては、次のリンクを参照してください。

[https://www.cisco.com/c/dam/en\\_us/about/doing\\_business/trust-center/docs/cisco-secure-boot-product-list.pdf](https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-boot-product-list.pdf)

## 回避策

この脆弱性に対処する回避策はありません。

[Cisco IOS デバイスの強化ガイドにデバイスを強化して管理アクセスのセキュリティを確保する方法が記載されています。](#)このドキュメントの推奨事項に従えば、この脆弱性の攻撃対象領域が縮小されます。

## 修正済みソフトウェア

修正済みソフトウェアリリースの詳細については、本アドバイザーの「脆弱性のある製品」セクションに記載されている Cisco Bug ID を参照してください。

シスコでは、このアドバイザーに記載された脆弱性に対処する無償の[ソフトウェア アップデートを提供する予定です](#)。お客様がインストールしたりサポートを受けたりできるのは、ライセンスをご購入いただいたソフトウェア バージョンとフィーチャ セットに対してのみとなります。その

ようなソフトウェアアップグレードをインストール、ダウンロード、アクセスまたはその他の方法で使用した場合、お客様は以下のリンクに記載されたシスコのソフトウェアライセンスの条項に従うことに同意したことになります。

<https://www.cisco.com/c/en/us/products/end-user-license-agreement.html>

また、お客様がソフトウェアをダウンロードできるのは、ソフトウェアの有効なライセンスをシスコから直接、あるいはシスコ認定リセラーやパートナーから取得している場合に限りです。通常、これは以前購入したソフトウェアのメンテナンスアップグレードです。無償のセキュリティソフトウェアアップデートによって、お客様に新しいソフトウェアライセンス、追加ソフトウェアフィチャセット、またはメジャーリビジョンアップグレードに対する権限が付与されることはありません。

ソフトウェアのアップグレードを検討する際には、[シスコのセキュリティアドバイザリおよびアラート ( Cisco Security Advisories and Alerts ) ] ページで入手できるシスコ製品のアドバイザリを定期的に参照して、侵害を受ける可能性と完全なアップグレードソリューションを確認してください。

いずれの場合も、アップグレードするデバイスに十分なメモリがあること、および現在のハードウェアとソフトウェアの構成が新規リリースで引き続き正しくサポートされていることを十分に確認してください。不明な点については、Cisco Technical Assistance Center ( TAC ) もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

## サービス契約をご利用でないお客様

シスコから直接購入したが Cisco Service Contract をご利用いただいていない場合、また、サードパーティベンダーから購入したが修正済みソフトウェアを POS から入手できない場合は、Cisco TAC に連絡してアップグレードを入手してください。

<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

無償アップグレードの対象製品であることを証明していただくために、製品のシリアル番号と、本アドバイザリの URL をご用意ください。

## 不正利用事例と公式発表

この脆弱性は、2019 年 5 月 13 日に Red Balloon Security 社によって公開されました。

Cisco Product Security Incident Response Team ( PSIRT ) は、Cisco ASR 1001-X でこの脆弱性を示す概念実証コードの存在を認識しています。今のところ、この概念実証コードが公開されているという情報はありません。

このアドバイザリで説明されている脆弱性の悪用に関する情報は Cisco PSIRT に寄せられていません。

## 出典

この脆弱性をシスコに報告し、情報公開にご協力いただいた Red Balloon Security 社の Jatin Kataria 氏 (主任科学的研究員)、Richard Housley 氏 (科学的研究員)、および Ang Cui 博士 (主任研究員) に感謝いたします。

## URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot>

## 改訂履歴

バージョン	説明	セクション	ステータス	日付
1.17	一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Final	2019年11月20日
1.16	一部の製品の修正バージョンが更新されました。	脆弱性が存在する製品	Final	2019年9月6日
1.15	脆弱性が存在する製品のリストを更新。	脆弱性が存在する製品	Final	2019年9月3日
1.14	脆弱性が存在する製品のリストを更新。	脆弱性が存在する製品	Final	2019年8月21日
1.13	一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Final	2019年8月2日
1.12	一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Final	2019年7月17日

バージョン	説明	セクション	ステータス	日付
1.11	一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Final	2019年6月28日
1.10	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Final	2019年6月17日
1.9	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。ドキュメントのステータスを最終版に変更。アドバイザリが更新されることを示した文を削除（概要および脆弱性のある製品）。	概要および脆弱性のある製品	Final	2019年6月10日
1.8	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Interim	2019年5月30日
1.7	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。セキュアブートをサポートするシスコ製品リストのリンクを追加。	脆弱性が存在する製品、詳細	Interim	2019年5月23日
1.6	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Interim	2019年5月22日
1.5	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Interim	2019年5月20日
1.4	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Interim	2019年5月16日
1.3	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在	Interim	2019年5月15日

バージョン	説明	セクション	ステータス	日付
		する製品		日
1.2	脆弱性が存在する製品のリストを更新。一部の製品向けに修正プログラムの提供日を更新。	脆弱性が存在する製品	Interim	2019年5月14日
1.1	脆弱性が存在する製品のリストを更新。Cisco Trustworthy テクノロジーのデータシートのリンクを追加。	脆弱性が存在する製品、詳細	Interim	2019年5月13日
1.0	初回公開リリース	—	Interim	2019年5月13日

## 利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。

本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意識を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。

## 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。