

نم ةيساسأل ةمظنأل ىلع جماربلا ةيقرت عيرسلل ءدبلل ليلد: ASR1000 ةلسلسلا

تايوتحمل

[ةمدقملا](#)

[ةيساسأل تابلطتملا](#)

[ةيساسأ تامولعم](#)

[Cisco IOS XE ةيقرت تاراسم](#)

[ةيقرتلل لبق امرايخا ةمئاق](#)

[ةماعلا ةيقرتلل تاوطخ](#)

[Cisco IOS XE Software جمانب ةيقرت ةيلمع](#)

[تثبيت تالعضو](#)

[\(SLP\) ةسايسلل مادختساب يكذلا صيخرتلل](#)

[ASR1000 ةيظمنلل تادحولل Cisco IOS XE نم موعدم رادصلل](#)

ةمدقملا

دنع تاسرامملا لصفأو ةفورعلملا تارادصلل او ةيساسأل تارابتعالا دنتسملا اذه فصلي
يتاذلل مكحتلا عضو في Cisco ASR 1000 Series هجوم جمانب ةيقرت

ةيساسأل تابلطتملا

تابلطتملا

ةيلالاتلا عيضاوملاب ةفرعم كيذل نوكت نأب Cisco يصوصت

- Cisco نم IOS® XE جمانب
- نايساسأل هترادلو هجوملا نيوكت

ةمدختسملا تانوكملا

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجالا نم دنتسملا اذه في ةدراولا تامولعملل عاشنإ مت
تناك اذا. (يضايرتفا) حوسمم نيوكتب دنتسملا اذه في ةمدختسملا ةزهجالا عيجم تادب
رما يأل لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا دي قكتكبش

ةيساسأ تامولعم

ثدحأل تارادصلإل او Cisco IOS XE 17.x إلى Cisco ASR 1000 Series هجوم ةيقرت نمضت تاوطخل ليلدل اذه حضوي .ءادلأ تانيسحتو نامأل تانيسحتو تازيمل ثدحأ نم ةدافتسالا ROMmon (ROM تارابتعاو ،ةميدقل تارادصلإل ةتقؤمل تايقرتل كلذ في امب ،ةيرورضلإ يكلذل صيخرتلل او (ناديمل في ةجرمل لل لباق ةباوب فيفص) FPGA و (Monitor

Cisco IOS XE ةيقرت تاراسم

ةيجمر ب ك يلع سسؤي ةصنم ASR1000 sery ل حارتقا رمم نيسحتل ةلواط اذه صخل ي:
ةغيص

رادصلإل يلاحلإ	مقر ةتقؤمل ةوطخل 1	2 مقر ةتقؤمل ةوطخلإ	ةوطخلإ ةريخأل
3.x/16 (1-8).x	16.9.x (RP2) (يرخأ زرت) و 16.12.x	صيخارت مادختسإ ةلاح في طقف (17.9.x) (ةطقل ذخأ متي ال PAK/RTU،	ثدحأ و 17.12
16.(9-12).x	رفوتم ريغ	صيخارت مادختسإ ةلاح في طقف (17.9.x) (ةطقل ذخأ متي ال PAK/RTU،	ثدحأ و 17.12

اذهو .تازيمل معد و أفاوثلل ةطيسو تايقرت مدقلأ تارادصلإل ضعب بلطتت :مهم اذه اذامل ةيقرتل دعب ام لمعو حيحص لكشب يساسأل ماظنل ديهمت نمضي

ةماه تاظحال م

PAK صيخرت ةطقل

- و 17.12.1a Cisco IOS XE إلى ةيقرتل ديرتو ةطقل نوب PAK صيخرت كيدل ناك اذا عضوب ماظنلل حامسلل (17.9.x) تقؤم رادصلإل إلى ةيقرتلل أو كيلع بجي ف ،ثدحأ رادصلإ — (DLC) زاهجل رشؤم ةطساوب ليوحتل تايلمع لامكإ و PAK صيخرتل ةيئاقلت ةطقل فدهل رادصلإل إلى ةيقرتلل م ث
- .ليصافت يلع لوصحلل PAK صيخارتب ةصاخلا تاقللل و [FN-74148](#) إلى عجار

ةفيعضل ةرفشلل لامهإ

Cisco IOS XE 17.11.1a نم ادب

- ةمومد دعتم لو 5 و 2 و 1 DH تاعومجمو MD5 و 3DES و DES لامهإ مت
- كلذ نم ادب DH Groups 14+ و SHA و AES مدختسأ
- اضيأ ةلمهم ESP-GMAC تاليوحت
- .ليصافت يلع لوصحلل [FN-72510](#) عجار



Cisco IOS XE إلى جم انربل ةيقرت عارجا متو ةلمهم تارفش نيوكت مت اذا :ريذحت



مداخل ليطعت هنع جتننيو IPsec قفن ضوافت لشفي، ثدحأ وأ 17.11.1a قفاوتل ليطعتب مق، ليجرتل اناثأ فيعض ريفشت مادختسإ يف اتقؤم رارمتسالل ديهمتل اداعإو Crypto Engine Compliance Shield رمأل عم CSDL عم

ةيقرتل لباق ام رايتخإ ةمئاق

- (انكمم كلذ ناك اذا) ةيلحمل صيخارتلاو ليلالحال نيوكتلل يطايتحال خسنلا
- ةتقؤملا ديهمتلا ةركاذ يلعتياباجيج 2 نعلقت ال ةرح ةحاسم رفوت نم دكأت (bootflash)
- لمعلال نعلقوتلل ةقيقد 20 ىلإ 15 نم صيصخت
- ةيقرتل راسم يف ةينعمل تارادصالا عيمل ةلصل تاذ رادصالا تاطحال عجار

ةماعلا ةيقرتل تاوطخ

ثدحأ رادصالا وأ 17.12 ىلإ Cisco IOS XE 3.x/16.(1-8).x نم: أ راسملا

1. (ROMmon [ةيقرت](#) عجار) رمأل مزلا اذا ROMmon ةيقرتب مق
2. ىرخأل زطلل 16.12.x وأ (ASR 1000-RP2 ج) Cisco IOS XE 16.9.x ىلإ ةيقرتل
3. (FPGA/CPLD [ةيقرت](#) عجار) رمأل مزلا اذا FPGA ةيقرت
4. دنع، Cisco IOS XE 17.9.x ىلإ ةيقرتلاب مق: ةطقل نودب PAK صيخارت مادختسإ مت اذا زاهجال يلعت ادامتعا ليوحتلا ةيلمع لمكيو [PAK ةطقل](#) ايئاقلت ماظنلا [نخأي](#)، ةيقرتل (DLC).
5. (ثدحأل وأ Cisco IOS XE 17.12) فدهلا رادصالا ىلإ ةيقرتلاب مق

ثدحأ رادصالا وأ 17.12 ىلإ Cisco IOS XE 16.(9-12).x نم: ب راسملا

1. (ROMmon [ةيقرت](#) عجار) رمأل مزلا اذا ROMmon ةيقرتب مق
2. (FPGA/CPLD [ةيقرت](#) عجار) رمأل مزلا اذا FPGA ةيقرت
3. دنع، Cisco IOS XE 17.9.x ىلإ ةيقرتلاب مق: ةطقل نودب PAK صيخارت مادختسإ مت اذا زاهجال يلعت ادامتعا ليوحتلا ةيلمع لمكيو [PAK](#) نم ةطقل [ايئاقلت](#) ماظنلا [نخأي](#)، ةيقرتل (DLC).
4. (ثدحأل وأ Cisco IOS XE 17.12) فدهلا رادصالا ىلإ ةيقرتلاب مق

ةبولطم ROMmon ةيقرت

هجوم يف ةنيعم ةزهجأ تادحو ىلعت تبثمل ديهمتلا ليمحت ةادل تابثال جمانربلا وه ROMmon Cisco IOS نم ثدحأ روصل اهل يغشتو ةزهجال ديهمت ةيناكإ ةيقرتل نمضت. Cisco IOS XE 17.x.

17.15(4r): ريرقتلا اذه ةباتك تقوي ف هب صوملا رادصالا



ASR 1001- ىلإ ةدوعلا كنكمي ال، ثدحأل وأ ROMmon 17.3(1r) ىلإ ةيقرتل دعب: ريدحت



يأىلىع قىباس رادصلإلى عوچرلا كنكمي ال، 17.15(4r) لىل ROMmon ةيقرت دعب :ريذحت
ي.ساسأ ماظن/ةقاطب

- جم انربلا رادصلإلى عچرا) RP ةدحو لىل ع تبثمل يلا لال ROMmon رادصلإلى نم ققحت
(جارخإلى لفسأ ي ف "تباثلا
<#root>

Router#

show platform

<...>

Slot	CPLD Version	Firmware Version
------	--------------	------------------

0	19060309	16.9(4r)
	R0	19060309
		16.9(4r)
		<<<<<
F0	19060309	16.9(4r)

- .ةيقرتلا عم ةعباتملاب مقف، 17.3(1r) نم مدقأ كب صاخلا رادصلإلى ناك اذا

ROMmon ةيقرت تاوطخ

bootflash. لىل ROMmon ةروص خسنا 1. ةوطخل

copy tftp: bootflash:

ةروشنملا ةميقلال قباطي ROMmon ةروصل MD5 يرابتخالا عومجملا نأ نم ققحت 2. ةوطخل
جماربلال ليزنت ةحفص لىل فلملا اذهل

verify /md5 bootflash:asr1000-rommon.1715-4r.SPA.pkg

ROMmon ةشاش ةيقرت 3. ةوطخل

```
upgrade rom-monitor filename bootflash:asr1000-rommon.1715-4r.SPA.pkg all
```



Upgrade rom-monitor all، ف لمل مسا رب ع 17.15(4r) ل ROMmon ةيقرت دن ع :ةطخال م hw<f0/F1> ةيطم نل ةدحول ةحت ف مادختساب ايودي ESP تاقاطب ليحت ةداع اب الوأ مق لك يهل ليحت ةداع اب مق ، قفاوم ةلاح ل تاقاطب الوصو درجم ب . ليحت ةداع عم ةدمل ةلطعم ESP ةيطم نل ةدحول لظت . ليحت ةداع ةزي م مادختساب لمك ل اب . دادر تسال انا ثا ةقيقد 15 ل لصت .



ع مجت متي — ROMmon ثيحت متي ال ، ASR1000-MIP100 ل ةبسننل اب :ةطخال م Upgrade rom-monitor رمأل م عدل دمعتم لكشب 17.15(4r) عضولا ي ف 16.3(2r) رادصلال ع قوتمل كولسل الو اذهو . filename all)

دراومل :

- [ROMmon ةيقرت ليلد](#)
- [ROMmon 17.15\(4r\) لي زنت](#)

FPGA/CPLD ةيقرت

تازيم ةرادا ل ع (ةجمر ب لل لباقلا دق عمل ا يقطنم ل زاهجلا) CPLD و FPGA تارادصل لمعت عا طخا ثودح ي ف ةمي دقلا و ا ةحيصلال ريغ تارادصلال ببستت دق . يوتسم ل ةضفخنم ةزهجال Cisco IOS XE نم ثدحا روص عم زاهجلاب ل طع ثودح و ا ديهمتلا ي ف

CPLD/FPGA رادصل ديكا ةي ف ي ك

- ةي لالال CPLD/FPGA تارادصل نم ققحتلل ةجمر ب لل لباقلا show all رمأ ليغشتب مق . ةيطم ن ةدحول لك
- رمأ ةصنم ضرع نم جاتنل نم يلفسلال مسقلال ي ف اضيأ ةغيص CPLD ل ضرعي

CPLD/FPGA ةيقرت متي تم

1.ةيقرتلا مزلي هنإف ،17071402 نم مدقأ FPGA رادصإ ناك اذإ ASR 1000-RP2 لوكوتورب

17071402 نم مدقأال FPGA تارادصإ وأ 16.9(5r) نم مدقأال تارادصإال ىلع رذعتي :ةظالم [CSCvm90995](#) id قب cisco تيأر .تيابايج 1 نم ربكأال IOS XE روص ديهمت

ىصوملا رادصإال نم مدقأ CPLD/FPGA ناك اذإ ةيقرتلا :ىرخأال ةيساسأال ةمظنأال •
هانأ هب

اهب ىصوملا تارادصإال

لكل FPGA و CPLD نم لكب ةصاخلا ليزنتلا طباورو اهب ىصوملا تارادصإال لودجلا اذه درسي
ASR 1000 ماطن

ةصنملا	CPLD	FPGA	ليزنت
ASR 1000-RP2	14111801	18102401	ليزنت
ASR 1000-RP3	19091111	—	ليزنت
ASR1001-X	19060309	—	ليزنت
ASR1002-X	14012203	20034	ليزنت
ASR1001-HX	19030215	16051716	ليزنت
ASR1002-HX	19030211	15102108	ليزنت

يساسأال ماطنلاب ةصاخ تاظحالم

• ةادأ - bin . فلم ىلإ ريشت تاظابترالا ليزنت ASR1002-HX و ASR1001-HX و ASR1001-X
ىلع لمعي يذلا Cisco نم نمآال ديهمتلا زاهج) [CVE-2019-1649](#) جلاعت ةصاخ FPGA ةيقرت
عجار .ROMmon ةبلاطم ةذفان نم هليغشت بجي .(ةينمأال طاقنلاب بعالتلا
[.ةيليصفتللا تاميلاعتلا](#)

• جامارب فلم ىلإ ريشت تاظابترالا ليزنت ASR1002-X و ASR1000-RP3 و ASR1000-RP2
ةيقرتلا تاوطخ .pkg . قيسنتب يسايق تباث

bootflash. ىلإ ةروصلا خسنا 1. ةوطخلا

copy tftp: bootflash:

ةزهجالل ةجمربلل لباقلا نوكملا ةيقرت 2. ةوطخلا

```
upgrade hw-programmable fpga filename bootflash:<hw-programmables-image.pkg> r0
```

Cisco IOS XE Software جمانرب ةيقرت ةيلمع

ىل Cisco IOS XE رادصلال ةيقرت ةيلمع بلطتت ،كيذل يلالال جمانربال رادصلال عاناب
ةرشابم ةيقرت نوكت دق وأ ةتقؤم ةيقرت ةوطخ 17.x رادصلال

مسقلا اذه يف نييرايلال الك فصومت ي

ةتقؤملا ةوطخلالاب ةيقرتلا: أراسملا

Cisco IOS XE 3.x وأ 16.(1-8).x نم يلالال رادصلال ناك اذا راسملا اذه مدختسأ: ةطحال م

ةيقرتلا تاوطخ

ققحتلالاو bootflash ىل ةتقؤملا ةروصلال خسنا 1. ةوطخلال

```
copy tftp://
```

```
bootflash:  
verify /md5 bootflash:
```

ةتقؤملا ةروصلال ديهمتلا تاملعم نييعتب مق 2. ةوطخلال

```
configure terminal  
no boot system  
boot system bootflash:
```

```
boot system bootflash:
```

```
end  
write memory
```

هوليمحت ةداعإو نيوكتال لجس نيي عت 3. ةوطخال

```
configure terminal
config-register 0x2102
end
write memory
reload
```

صيخرتال ةلاحو فئاطول نم ققحت ،تقؤملا رادصإلا في هجوملا ديمت درجمب

ققحتلالو bootflash إلى ةيئاهنلا ةروصلال خسنأ 4. ةوطخال

```
copy tftp://
```

```
bootflash:
verify /md5 bootflash:
```

لليمحتال دعأو نيوكتال ظفحا مث ،ةيئاهنلا ةروصلال إلى ديمتال نايب شي دحتب مق 5. ةوطخال

```
configure terminal
no boot system
boot system bootflash:
```

```
boot system bootflash:
```

```
end
write memory
reload
```

Cisco IOS XE 17.x إى ةيقرتال :ب راسملا



نوكت Cisco IOS XE 16.(9-12).x نم يلحال رادصلإا ناك اذا راسملا اذه مدختسأ: ةطحال
Cisco IOS XE 17.x إلإ ةرشابملا ةيقرتل عم ةقفاوتم تارادصلإا هذه

PAK و ثدحال وأ Cisco IOS XE 17.12 وه فدهل نكي مل ام ةبولطم ةتقؤم ةوطخ دجوت ال
إلإ ةتقؤملا ةيقرتللاب صوي، ةلحال هذه يف - ةطقل ذخأ نود اهمادختسإ مت يتل
[PAK. ةطقل عيمجت نكمي يلاتلابو](#)، ال وأ 17.9.x

ةيقرتل تاوطخ

ققحتلالو bootflash إلإ ةيئاهنلا ةروصلل خسنا 1. ةوطخل

```
copy tftp://
```

```
bootflash:  
verify /md5 bootflash:
```

ديهمتل ةروص نيوكت 2. ةوطخل

```
configure terminal  
no boot system  
boot system bootflash:
```

```
boot system bootflash:
```

```
end  
write memory
```

هليمحت ةداعإو نيوكتل لجس نييعت 3. ةوطخل

```
configure terminal  
config-register 0x2102  
end  
write memory  
reload
```

تي بثلت لعضو

لكشب تي بثلثال عضو في एसएसएल एमप्लानأل عي مج نحش م تي cisco IOS XE 17.15.1a، ن م
تي بثلثال رم اوأ مادختساب ضا فإل او قي قرتل او دي هم ثل كن كم ي. ي ضا رت فا

بولسا بكري في ضفخي ونسحي ،بولسا بكري نأ بولسا قمزح نم لي وحتلا ىلع تاداشرا
رما بكري لمعتسي قيچمربلا بكري

(SLP) ةسايسل مادختساب يكذل صيخرتلا

Cisco IOS XE تارادص ال اي ف اي مازال ةسايس ال مادختساب ي كذل صيخرت ال حبصي : بل طتم ال .
ش دحل تارادص ال او 17.3.2

قاحلالا ليلدو Cisco SLP ىلع ةماع قرظن :عجرملا

ASR1000 هي طم ن ل ا ت ا د ح و ل ل Cisco IOS XE ن م م و ع د م ر ا د ص ا ر خ آ

نم موع دم رادصا رخ Cisco IOS XE	عزجلا فرعم
17,18,x	ASR1000-MIP100
17,18,x	EPA-1x100GE EPA-QSFP-1x100GE EPA-2x40GE EPA-18X1GE EPA-10x10GE
17,18,x	ASR1000-ESP100-X ASR1000-ESP200-X
17,18,x	ASR1000-RP3
17,15,x	ASR1000-ESP100 ASR1000-ESP200

17,9,x	ASR1000-RP2
17,9,x	ASR1000-SIP40
17,9,x	ASR1000-6TGE ASR1000-2T+20X1GE



ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا