Cisco IOS XR出力パケットネットワークインターフェイスアライナーの割り込みによるDoS脆弱性

High

アドバイザリーID : cisco-sa-xrncs-epni-int-dos-TWMffUsN
CVE-2026-20118
初公開日 : 2026-03-11 16:00
バージョン 1.0 : Final
CVSSスコア : 6.8
回避策 : No workarounds available
Cisco バグ ID : CSCws66900 CSCws66892

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

NC57ラインカードとCisco NCS 5700ルータを使用したCisco Network Convergence System(NCS)5500シリーズ用のCisco IOS XRソフトウェアおよびサードパーティソフトウェア用のCisco IOS XRソフトウェアにおける出力パケットネットワークインターフェイス(EPNI)アライナーの割り込みの処理における脆弱性により、認証されていないリモート攻撃者がネットワーク処理ユニット(NPU)とASICを処理させ、トラフィックがを通過阻止するする可能性があります。

この脆弱性は、該当デバイスで大量のトランジットトラフィックが発生しているときにEPNI Alignerの割り込みがトリガーされる特定のケースでパケットが破損することに起因します。攻撃者は、該当デバイスのインターフェイスに、巧妙に細工されたパケットの連続フローを送信することにより、この脆弱性を不正利用する可能性があります。エクスプロイトに成功すると、攻撃者はパケットを大量に持続的に損失させ、その結果サービス妨害(DoS)状態が発生する可能性があります。

注：この脆弱性のアクティブなエクスプロイトが疑われる場合は、Cisco Technical Assistance Center(TAC)または契約したメンテナンスプロバイダーにお問い合わせください。

シスコはこのセキュリティアドバイザリのスコアが示すように、Security Impact Rating(SIR)をMediumではなくHighに設定しました。この変更が行われた理由は、影響を受けるデバイスが重要なネットワークセグメント内で動作しており、このセグメントでセキュリティ侵害が発生すると、重大な中断や漏洩が発生し、全体的なリスクが基本的な技術的な重大度を超えてしまう可能性があるからです。

シスコ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しています。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-xrncs-epni-int-dos-TWMffUsN

このアドバイザリは、Cisco IOS XRソフトウェアSecurity Advisoryバンドル公開の2026年3月リリースの一部です。アドバイザリとリンクの一覧については、Cisco Event Response: March 2026 Semiannual Cisco IOS XR Software Security Advisory Bundled Publication を参照してください。

該当製品

脆弱性のある製品

この脆弱性は、デバイス設定に関係なく、Cisco IOS XRソフトウェアの脆弱性のあるリリースを実行している次のシスコ製品に影響を与えます。

- 次の製品ID(PID)のNCS 5700シリーズラインカード
  - NC57-18DD-SE
  - NC57-24DD
  - NC57-36H-SE
  - NC57-36H6D-S
  - NC57-MOD-S
- NCS 5700シリーズ固定シャーシ（次のPIDを搭載）
  - NCS-57B1-5D24H-SE
  - NCS-57B1-5DSE-SYS
  - NCS-57B1-6D24-SYS
  - NCS-57B1-6D24H-S

サードパーティハードウェアにJericho 2 ASICが搭載されている場合、この脆弱性はサードパーティハードウェア用のCisco IOS XRにも影響を与えます。

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

該当するラインカードが取り付けられているかどうかを確認する

該当するラインカードがシステムにインストールされているかどうかを判別するには、show inventory CLIコマンドを使用して該当するラインカードのPIDを検索します。

```
<#root>

RP/0/RP0/CPU0:NCS_Router#

show inventory


Tue Feb 18 10:55:15.397 UTC
NAME: "0/0", DESCR: "NCS 5700 18x400GE Line Card with TCAM"

PID: NC57-18DD-SE

      , VID: V03, SN: JAE271602RT

NAME: "HundredGigE0/0/0/0", DESCR: "Cisco QSFP28 100G SR4 Pluggable Optics Module"
PID: QSFP-100G-SR4-S    , VID: V03, SN: INL270701RY

NAME: "FourHundredGigE0/0/0/18", DESCR: "Cisco QSFPDD 400G DR4 Pluggable Optics Module"
PID: QDD-400G-DR4-S     , VID: V02 , SN: INL27060SZ7

NAME: "0/1", DESCR: "NCS 5700 36x100GE 6x400GE Line Card"

PID: NC57-36H6D-S

      , VID: V01, SN: JAE27170FQG

NAME: "0/2", DESCR: "NCS 5700 2XMPA Scaled Line Card, MACSec"
PID: NC55-MOD-A-SE-S    , VID: V02, SN: JAE2714041Y

NAME: "GigabitEthernet0/2/0/4", DESCR: "Cisco SFP 1G 1000BASE-SX Pluggable Optics Module"
PID: SFP-GE-S           , VID: V01, SN: FNS11510HSN

NAME: "0/3", DESCR: "NCS 5700 36x100GE Line Card with TCAM"

PID: NC57-36H-SE

       , VID: V02, SN: JAE271406WC
```

脆弱性を含んでいないことが確認された製品

このアドバイザリの脆弱性のある製品セクションにリストされている製品だけがこの脆弱性の影響を受けることが知られています。

シスコは、この脆弱性が以下のシスコ製品には影響を与えないことを確認しました。

- IOS ソフトウェア
- IOS XE ソフトウェア
- 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たモデル以外のデバイスで実行されているIOS XRソフトウェア
- NX-OS ソフトウェア

詳細

デバイス上のEPNI Aligner割り込みは、この脆弱性を使用して攻撃が試みられた証拠である可能

性があります。割り込みを確認するには、show asic-errors fia all location "" | begin Alignerコマンドを使用します。

```
<#root>

RP/0/RP0/CPU0:NCS_Router#

show asic-errors fia all location 0/4/CPU0 | begin Aligner


<Output Snipped>
Name : EPNI_0.Interrupt_Register.

AlignerTransmitSizeAboveThInt


Leaf ID : 0x36030011
Error count :

2


Last clearing : DDD MMM X HH:MM:SS YYYY
Last N errors :

2


------------------------------------------------------------
First N errors.
@Time, Error-Data
----------------------------------------
<Output Snipped>
Error description: Check for misconfiguration in ETPP|None
<Output Snipped>
Error description: Check for misconfiguration in ETPP|None
```

このコマンドの出力のNameフィールドにAlignerTransmitSizeAboveThIntが含まれている場合は、EPNI Aligner割り込みが発生しています。

ただし、修正済みリリースのCisco IOS XRソフトウェアを実行しているデバイス、またはこの脆弱性に対処するSMUがインストールされているデバイスは、割り込みを正常に処理し、この脆弱性の影響を受けません。 デバイスでCisco IOS XRソフトウェアの脆弱なリリースが実行されている場合、EPNI Alignerの割り込みによりDoS状態が発生する可能性があります。

ネットワーク内のPIDに影響を与えるすべてのお客様は、適切なSMUをインストールするか、修正済みのCisco IOS XRソフトウェアリリースにアップグレードすることを強く推奨します。詳細については、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

回避策

この脆弱性に対処する回避策はありません。

修正済みソフトウェア

シスコでは、回避策や緩和策（該当する場合）は、修正済みソフトウェアリリースへのアップグレードが利用可能になるまでの一時的な解決策であると考えています。この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するために、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

次の表では、左の列にシスコ ソフトウェア リリースまたはトレインを記載しています。右側の列は、リリース（トレイン）がこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこの脆弱性に対する修正を含む最初のリリースを示しています。

Cisco IOS XR ソフトウェアリリース	First Fixed Release（修正された最初のリリース）
7.8.2 以前	影響なし。
7.9	修正済みリリースに移行するか、SMUを適用します。
7.10	修正済みリリースに移行するか、SMUを適用します。
7.11	修正済みリリースに移行するか、SMUを適用します。
24.1	修正済みリリースに移行するか、SMUを適用します。
24.2	修正済みリリースに移行するか、SMUを適用します。
24.3	修正済みリリースに移行するか、SMUを適用します。
24.4	修正済みリリースに移行するか、SMUを適用します。
25.1	修正済みリリースに移行するか、SMUを適用します。
25.2	脆弱性なし
25.3	脆弱性なし
25.4	脆弱性なし
26.1	脆弱性なし

この問題に対処するため、次のSMUが公開されています。

Cisco IOS XR ソフトウェア リリース	Cisco Bug ID	SMU 名
7.9.2	CSCws66900	ncs5500-7.9.2.CSCws66900 ncs5700-7.9.2.CSCws66900 iosxrwbd-7.9.2.CSCws66900
7.10.2	CSCws66892	ncs5500-7.10.2.CSCws66892 ncs5700-7.10.2.CSCws66892
7.11.2	CSCws66900	ncs5500-7.11.2.CSCws66900

Cisco IOS XR ソフトウェア リリース	Cisco Bug ID	SMU 名
		ncs5700-7.11.2.CSCws66900 iosxrwbd-7.11.2.CSCws66900
7.11.21	CSCws66900	ncs5500-7.11.21.CSCws66900 ncs5700-7.11.21.CSCws66900
24.1.2	CSCws66892	ncs5500-24.1.2.CSCws66892 ncs5700-24.1.2.CSCws66892
24.2.2	CSCws66892	ncs5500-24.2.2.CSCws66892 ncs5700-24.2.2.CSCws66892
24.2.21	CSCws66900	ncs5500-24.2.21.CSCws66900 ncs5700-24.2.21.CSCws66900
24.3.2	CSCws66900	ncs5500-24.3.2.CSCws66900 ncs5700-24.3.2.CSCws66900
24.4.2	CSCws66900	ncs5500-24.4.2.CSCws66900 ncs5700-24.4.2.CSCws66900
25.1.2	CSCws66900	ncs5500-25.1.2.CSCws66900 ncs5700-25.1.2.CSCws66900

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例やその公表は確認しておりません。

出典

この脆弱性は Cisco Cisco Technical Assistance Center（TAC）サポートケースの解決中に発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrncs-epni-int-dos-TWMffUsN

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026年3月11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、単独の転載や意訳を施した場合、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。