Multiple Vulnerabilities in Cisco NX-OS-Based Products

Advisory ID：cisco-sa-20130424-nxosmulti

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-nxosmulti/

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。

Revisio 1.2

Last Updated 2013 April 26 19:40 UTC (GMT)

For Public Release 2013 April 24 16:00 UTC (GMT)

目次

要約

Cisco Nexus、Cisco Unified Computing System（UCS）、Cisco MDS 9000 シリーズ マルチレイヤ スイッチ、Cisco 1000 シリーズ Connected Grid ルータ（CGR）はすべて Cisco NX-OS オペレーティング システムをベースとしています。これらの製品は、次の脆弱性のうち少なくとも 1 つの影響を受けます。

- Cisco NX-OS ベースの製品の Cisco Discovery Protocol に関する複数の脆弱性
- Cisco NX-OS ソフトウェアの SNMP および License Managerのバッファ オーバーフローに関する脆弱性
- Cisco NX-OS ソフトウェアの SNMP バッファ オーバーフローに関する脆弱性
- Cisco NX-OS ソフトウェアのジャンボ パケットの DoS（サービス拒否）に関する脆弱性

シスコはこれらの脆弱性に対応するための無償ソフトウェア アップデートを提供しています。

このアドバイザリは、次のリンクで確認できます。
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-nxosmulti/

該当製品

Cisco NX-OS ソフトウェア高速ルーティングおよびスイッチング プラットフォームを稼働する、またはこれをベースとするシスコ製品は、本アドバイザリで説明する脆弱性のうち少なくとも 1 つの影響を受けます。

脆弱性が認められる製品

次の製品には脆弱性が存在します。

Cisco UCS 6100 = Cisco Unified Computing Server ファブリック インターコネクト 6100 シリーズ デバイス
Cisco UCS 6200 = Cisco Unified Computing Server ファブリック インターコネクト 6200 シリーズ デバイス
Cisco Nexus 7000 = Cisco Nexus 7000 シリーズ デバイス
Cisco Nexus 5000 = Cisco Nexus 5010 および Cisco Nexus 5020 デバイス
Cisco Nexus 5500 = Cisco Nexus 5500 シリーズ デバイス
Cisco Nexus 4000 = Cisco Nexus 4000 シリーズ ブレード デバイス
Cisco Nexus 3000 = Cisco Nexus 3000 シリーズ デバイス
Cisco Nexus 1000v = Cisco Nexus 1000v 仮想スイッチおよび 1010 仮想サービス アプライアンス
Cisco MDS 9000 = Cisco MDS 9000 マルチレイヤ スイッチ/ディレクタ ファミリ デバイス
Cisco CGR 1000 = Cisco Connected Grid ルータ 1000 シリーズ デバイス

次の表に各脆弱性の影響を受ける製品を示します。

	Cisco Nexus 7000	Cisco Nexus 5000	Cisco Nexus 5500	Cisco Nexus 4000	Cisco Nexus 3000	Cisco Nexus 1000V	Cisco MDS 9000	C
Multiple CDP Buffer Overflow CVE-2013-1178	X	X	X	X	X	X	X	
SNMP & License Manager Buffer Overflow CVE-2013-1179	X						X	
SNMP Buffer Overflow CVE-2013-1180	X						X	
Jumbo Frame Denial of Service CVE-2013-1181			X		X			
Recommended Software	5.2(9)/6.1(1)	5.2(1)N1(4)	5.2(1)N1(4)	4.1(2)E1(1j)	5.0(3)U5(1e)	4.2(1)SV2(1.1)	5.2(8)	2

注：上の表の Recommended Software に記載されたリリースは、各プラットフォームに影響を与

える脆弱性をすべて解決します。

脆弱性が認められない製品

Cisco Nexus 3548 スイッチは本ドキュメントに記載された脆弱性の影響を受けません。

Cisco Nexus 6000 シリーズ デバイスは本ドキュメントに記載された脆弱性の影響を受けません。

他のシスコ製品においてこの脆弱性の影響を受けるものは、現在確認されていません。

詳細

Cisco NX-OS ベースの製品の Cisco Discovery Protocol に関する複数の脆弱性

Cisco NX-OS ベースのデバイスには、Cisco Discovery Protocol（CDP）サブシステムに複数のバッファ オーバーフローに関する脆弱性があります。これらの脆弱性によって、認証されていない近接した攻撃者が高い特権を使用して任意のコードを実行する可能性があります。これらの脆弱性は、不正な Cisco Discovery Protocol パケットに対する適切な処理の失敗に起因します。攻撃者は不正な Cisco Discovery Protocol パケットを該当デバイスに渡すことにより、これらの脆弱性を不正利用する可能性があります。これらの脆弱性の不正利用に成功した場合、攻撃者は高い特権を使用して任意のコードを実行する可能性があります。

Cisco Discovery Protocol はデータリンク層（レイヤ 2）で動作するので、この脆弱性を不正利用するためには、攻撃者はイーサネット フレームを該当デバイスに直接送信する必要があります。これは、該当デバイスがブリッジ型ネットワークに組み込まれている場合や、ネットワーク ハブのようなパーティションがないデバイスに接続されている場合に可能になります。

この脆弱性は、次の Cisco Bug ID として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-1178 が割り当てられています。

Cisco Bug ID：

- **UCS 6100/UCS 6200** ：CSCtu10630（登録ユーザ専用）
- **Nexus 7000/MDS 9000**：CSCtu10551（登録ユーザ専用）
- **Nexus 5000/Nexus 5500**：CSCtu10550（登録ユーザ専用）
- **Nexus 4000**：CSCtw56581（登録ユーザ専用）
- **Nexus 3000**：CSCtu10548（登録ユーザ専用）
- **Nexus 1000v**：CSCtu10544（登録ユーザ専用）
- **CGR 1000**：CSCuf61275（登録ユーザ専用）

Cisco NX-OS ソフトウェアの SNMP および License Managerのバッファ オーバーフローに関する脆弱性

Cisco NX-OS ソフトウェア ベースのデバイスには、SNMP サブシステムにバッファ オーバーフローに関する脆弱性があります。認証されたリモートの攻撃者が、UDP ポート 161 経由で不正な SNMP クエリを送信することによってこの脆弱性を不正利用し、デバイスの SNMP コンポーネントと License Manager コンポーネントにバッファ オーバーフロー状態を引き起こす可能性があります。不正利用に成功した場合、攻撃者は高い特権を使用して任意のコードを実行する可能性があります。

SNMP はデフォルトで無効になっており、管理者が明示的に設定を行う必要があります。SNMP は主に UDP をベースとしたプロトコルであるため、この脆弱性の不正利用に TCP 3 ウェイ ハン

ドシェイクは不要であり、不正なリクエストにスプーフィングされた送信元が含まれる可能性があります。攻撃者は SNMP バージョン 1 およびバージョン 2 に設定されたコミュニティ文字列を知っている必要があります。また、デバイスに SNMP バージョン 3 が設定されている場合、不正利用には有効なユーザ名とパスワードも必要となります。

この脆弱性は SNMP over IPv4 および SNMP over IPv6 経由で引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCtx54830（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1179 が割り当てられています。

Cisco NX-OS ソフトウェアの SNMP バッファ オーバーフローに関する脆弱性

Cisco NX-OS ベースのデバイスには、SNMP サブシステムにバッファ オーバーフローに関する脆弱性があります。認証されたリモートの攻撃者が、UDP ポート 161 経由で不正な SNMP クエリを送信することによってこの脆弱性を不正利用し、デバイスの SNMP コンポーネントにバッファ オーバーフロー状態を引き起こす可能性があります。不正利用に成功した場合、攻撃者は高い特権を使用して任意のコードを実行する可能性があります。

SNMP はデフォルトで無効になっており、管理者が明示的に設定を行う必要があります。SNMP は主に UDP をベースとしたプロトコルであるため、この脆弱性の不正利用に TCP 3 ウェイ ハンドシェイクは不要であり、不正なリクエストにスプーフィングされた送信元が含まれる可能性があります。攻撃者は SNMP バージョン 1 およびバージョン 2 に設定されたコミュニティ文字列を知っている必要があります。また、デバイスに SNMP バージョン 3 が設定されている場合、不正利用には有効なユーザ名とパスワードも必要となります。

この脆弱性は SNMP over IPv4 および SNMP over IPv6 経由で引き起こされる可能性があります。

この脆弱性は、Cisco Bug ID CSCtx54822（ 登録ユーザ専用 ）として文書化され、CVE ID として CVE-2013-1180 が割り当てられています。

Cisco NX-OS ソフトウェアのジャンボ パケットの DoS（サービス拒否）に関する脆弱性

Cisco NX-OS ベースのデバイスには DoS（サービス拒否）に関する脆弱性が存在します。認証されていないリモートの攻撃者が、該当デバイスの管理インターフェイスにジャンボ フレーム パケットを送信することによって、デバイスのクラッシュとリロードが引き起こされる可能性があります。

この脆弱性は、ジャンボ パケットに対する不適切な入力検証に起因します。デバイスのスイッチング ファブリック経由で送信される大きいパケットがこの脆弱性を誘発することはありません。

この脆弱性は、次の Cisco Bug ID として文書化され、Common Vulnerabilities and Exposures（CVE）ID として CVE-2013-1181 が割り当てられています。

Cisco Bug ID：

- **UCS 6200**：CSCtx17544（登録ユーザ専用）
- **Nexus 5500**：CSCts10593（登録ユーザ専用）
- **Nexus 3000**：CSCtx95389（登録ユーザ専用）

脆弱性スコア詳細

シスコはこのアドバイザリでの脆弱性に対して Common Vulnerability Scoring System（CVSS）に基づいたスコアを提供しています。本セキュリティ アドバイザリでの CVSS スコアは、CVSS バージョン 2.0 に基づいています。

CVSS は、脆弱性の重要度を示唆するもので、緊急性および対応の優先度を決定する組織の手助けとなる標準ベースの評価法です。

シスコでは、基本評価スコア（Base Score）および現状評価スコア（Temporal Score）を提供しています。お客様はこれらを用いて環境評価スコア（Environmental Score）を算出し、自身のネットワークにおける脆弱性の影響度を知ることができます。

シスコは次のリンクで CVSS に関する追加情報を提供しています。

http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html

またシスコでは、各ネットワークにおける環境影響度を算出する CVSS 計算ツールを次のリンクで提供しています。

http://tools.cisco.com/security/center/cvssCalculator.x/

CSCtu10630, CSCtu10551, CSCtu10550, CSCtu10548, CSCtu10544, CSCtw56581, CSCuf61275 - Multiple Cisco Discovery Protocol Vulnerabilities in Cisco NX-OS-Based Products **Calculate the environmental score of**					
CVSS Base Score - **8.3**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Adjacent Network	Low	None	Complete	Complete	Complete
CVSS Temporal Score - **6.9**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtx54830 - Cisco NX-OS Software SNMP and License Manager Buffer Overflow Vulnerability **Calculate the environmental score of**					
CVSS Base Score - **9.0**					
Access Vecto	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact

r					
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCtx54822 - Cisco NX-OS Software SNMP Buffer Overflow Vulnerability Calculate the environmental score of					
CVSS Base Score - **9.0**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	Single	Complete	Complete	Complete
CVSS Temporal Score - **7.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

CSCts10593, CSCtx95389, CSCtx17544 - Cisco NX-OS Software Jumbo Packet Denial of Service Vulnerability Calculate the environmental score of					
CVSS Base Score - **7.8**					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Low	None	None	None	Complete
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

本ドキュメントに記載された Cisco Discovery Protocol に関する脆弱性のいずれかの不正利用に成功した場合、認証されていない近接した攻撃者が高い特権を使用して任意のコードを実行する可能性があります。

SNMP に関する脆弱性のいずれかの不正利用に成功した場合、攻撃者が高い特権を使用して任意のコードを実行する可能性があり、その結果として該当デバイスのセキュリティ侵害に至る恐れがあります。

ジャンボ パケットに関する脆弱性の不正利用に成功した場合、攻撃者がデバイスの再起動を引き起こす可能性があります。攻撃が持続すると、DoS 状態が続く可能性があります。

ソフトウェア バージョンおよび修正

ソフトウェアのアップグレードを検討する場合は、 http://www.cisco.com/go/psirt/ の Cisco Security Advisories, Responses, and Notices アーカイブや、後続のアドバイザリを参照して、起こりうる障害を判断し、それに対応できるアップグレード 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、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。

Nexus 7000

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	4.1(x) 4.2(x) 5.0(x) 5.1(x) 5.2(3a) and Prior 6.0(x)	5.2(4) 6.1(1)	5.2(9) 6.1(1)
SNMP & License Manager CVE-2013-1179	4.1(x) 4.2(x) 5.0(x) 5.1(x) 5.2(4) and Prior 6.0(x)	5.2(5) 6.1(1)	5.2(9) 6.1(1)
SNMP CVE-2013-1180	4.1(x) 4.2(x) 5.0(x) 5.1(x) 5.2(4) and Prior 6.0(x)	5.2(5) 6.1(1)	5.2(9) 6.1(1)

Nexus 5000/Nexus 5500

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	4.0(x) 4.1(x) 4.2(x) 5.0(x)	5.1(3)N1(1)	5.2(1)N1(4)
Jumbo Frame - Nexus 5500 CVE-2013-1181	4.0(x) 4.1(x) 4.2(x) 5.0(3)N2(1) and Prior	5.0(3)N2(2)	5.2(1)N1(4)

Nexus 4000

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	4.1(2)E1(1g) and Prior	4.1(2)E1(1h)	4.1(2)E1(1j)

Nexus 3000

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	5.0(3)U1(1x) 5.0(3)U1(2x) 5.0(3)U2(1) 5.0(3)U2(2x)	5.0(3)U3(1)	5.0(3)U5(1e)
Jumbo Frame CVE-2013-1181	5.0(3)U1(1x) 5.0(3)U1(2x) 5.0(3)U2(1) 5.0(3)U2(2x) 5.0(3)U3(1)	5.0(3)U3(2)	5.0(3)U5(1e)

Nexus 1000V

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	4.0(x) 4.2(1)SV1(4b) and Prior	4.2(1)SV1(5.1)	4.2(1)SV2(1.1)

MDS 9000

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	4.1(x) 4.2(x) 5.0(x) 5.2(3) and Prior	5.2(4)	5.2(8)
SNMP & License Manager CVE-2013-1179	4.1(x) 4.2(x) 5.0(x) 5.2(4) and Prior	5.2(5)	5.2(8)
SNMP CVE-2013-1180	4.1(x) 4.2(x) 5.0(x) 5.2(4) and Prior	5.2(5)	5.2(8)

Unified Computing System

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	1.0(x) 1.1(x) 1.2(x) 1.3(x) 1.4(x) 2.0(1x) and Prior	2.0(2m) 2.1(1a)	2.1.1e
Jumbo Frame - UCS 6200 CVE-2013-1181	1.0(x) 1.1(x) 1.2(x) 1.3(x) 1.4(x) 2.0(1t) and prior	2.0(1w)	2.1.1e

Connected Grid ルータ 1000 シリーズ

	Affected	First Fixed	Recommended
Multiple CDP CVE-2013-1178	CG1(4) CG1(5) CG3(1) CG3(2) CG3(3)	CG4(1)	CG4(1)

回避策

このアドバイザリに記載された脆弱性には、デバイス上での回避策がありません。

シスコはこれらの脆弱性の検出方法と不正利用の可能性を低減する方法を説明した「Applied Mitigation Bulletin」（AMB）をリリースしています。AMB「 *Identifying and Mitigating Exploitation of Multiple Vulnerabilities in Cisco NX-OS-Based Products*」は次のリンクで公開しています。
http://tools.cisco.com/security/center/viewAMBAlert.x?alertId=28737/

修正済みソフトウェアの入手

シスコはこのアドバイザリ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しています。ソフトウェアの導入を行う前に、お客様のメンテナンス プロバイダーにご相談いただくか、ソフトウェアのフィーチャ セットの互換性およびお客様のネットワーク環境の特有の問題をご確認ください。

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、ご購入いただいたフィーチャ 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 http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html に記載の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。

サービス契約をご利用のお客様

サービス契約をご利用のお客様は、通常のアップデート チャネルからアップグレード ソフトウェアを入手してください。ほとんどのお客様は、 Cisco.com の Software Navigator からアップグレード ソフトウェアを入手できます。 http://www.cisco.com/cisco/software/navigator.html

サードパーティのサポート会社をご利用のお客様

シスコ パートナー、正規販売代理店、サービス プロバイダーなど、サードパーティのサポート会社と以前に契約していたか、または現在契約しており、その会社からシスコ製品の提供または保守を受けているお客様は、該当するサポート会社に連絡し、正しい処置についてのサポートを受けてください。

回避策や修正の効果は、使用している製品、ネットワーク トポロジー、トラフィックの性質や組織の目的などに関するお客様の状況によって異なります。影響を受ける製品やリリースは多種多様であるため、回避策を実施する前に、対象ネットワークで適用する回避策または修正が最適であることを、お客様のサービス プロバイダーやサポート会社にご確認ください。

サービス契約をご利用でないお客様

シスコから製品を直接購入したもののシスコのサービス契約をご利用いただいていない場合、ま

たは、サードパーティ ベンダーから購入したものの修正済みソフトウェアを購入先から入手できない場合は、Cisco Technical Assistance Center（TAC）に連絡してアップグレード ソフトウェアを入手してください。

- +1 800 553 2447（北米からの無料通話）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

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。サービス契約をご利用でないお客様は TAC に無償アップグレードをリクエストしてください。

多言語による各地の電話番号、説明、E メール アドレスなどの TAC の連絡先情報については、Cisco Worldwide Contact を参照してください。
http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

不正利用事例と公式発表

Cisco Product Security Incident Response Team（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とその公表は確認しておりません。

次の脆弱性は、NX-OS ベースの製品に対する社内のセキュリティ評価中に発見されました。

- Cisco NX-OS ベースの製品の Cisco Discovery Protocol に関する複数の脆弱性
- Cisco NX-OS ソフトウェアの SNMP および License Managerのバッファ オーバーフローに関する脆弱性
- Cisco NX-OS ソフトウェアの SNMP バッファ オーバーフローに関する脆弱性

Cisco NX-OS ソフトウェア ジャンボ パケットの DoS 脆弱性は、お客様のサポート中に Cisco TAC によって発見されました。

この通知のステータス：FINAL

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を示唆するものでもありません。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。またシスコはいつでも本ドキュメントの変更や更新を実施する権利を有します。

後述する情報配信の URL を省略し、本アドバイザリの記述内容に関して単独の転載や意訳を実施した場合には、事実誤認ないし重要な情報の欠落を含む統制不可能な情報の伝搬が行われる可能性があります。

情報配信

このアドバイザリは次のリンクにある Cisco Security Intelligence Operations に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130424-nxosmulti/

また、このアドバイザリのテキスト版が Cisco PSIRT PGP キーによるクリア署名つきで次の E メールで配信されています。

- cust-security-announce@cisco.com

- first-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk

本アドバイザリに関する今後の更新は Cisco.com に掲載されますが、メーリング リストで配信されるとは限りません。更新内容については、本アドバイザリの URL でご確認ください。

更新履歴

Revision 1.2	2013-April-26	Updated summary table in Affected Products for clarification. Corrected UCS 6100/6200 information for jumbo frame vulnerability in summary table.
Revision 1.1	2013-April-24	Clarified affected platforms for certain vulnerabilities.
Revision 1.0	2013-April-24	Initial public release.

シスコ セキュリティ手順

シスコ製品におけるセキュリティの脆弱性の報告、セキュリティ事故に関するサポート、およびシスコからセキュリティ情報を入手するための登録方法の詳細については、Cisco.com の http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html を参照してください。この Web ページには、シスコのセキュリティ アドバイザリに関してメディアが問い合わせる際の指示が掲載されています。シスコ セキュリティ アドバイザリについては、すべて http://www.cisco.com/go/psirt/ で確認できます。