Cisco Integrated Management Controller Supervisor and Cisco UCS Director Remote File Overwrite Vulnerability

Advisory ID: cisco-sa-20150902-cimcs

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150902-cimcs

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。

Revision 1.0

For Public Release 2015 September 2 16:00 UTC (GMT)

目次

要約

Cisco Integrated Management Controller（IMC）Supervisor と Cisco UCS Director には、認証されていないリモート攻撃者が任意のシステム ファイルを上書きする可能性がある脆弱性が含まれており、結果として、システムが不安定になったり、サービス妨害（DoS）状態が発生するおそれがあります。

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ました。

これらの脆弱性に対しては回避策がありません。

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-20150902-cimcs

該当製品

脆弱性が存在する製品

この脆弱性は、以下の 2 つのシスコ製品に影響します。

- Cisco IMC Supervisor の 1.0.0.1 より前のソフトウェア バージョン
- Cisco UCS Director（旧称 Cloupia Unified Infrastructure Controller）の 5.2.0.1 より前のソフトウェア バージョン

脆弱性が存在しない製品

他のシスコ製品において、このアドバイザリの影響を受けるものは現在確認されていません。

詳細

Cisco IMC Supervisor と Cisco UCS Director の JavaServer Pages（JSP）の入力検証ルーチンの脆弱性により、認証されていないリモート攻撃者がシステムの任意のファイルを上書きする可能性があります。

この脆弱性は、特定の JSP ページでの不十分な入力サニタイズに起因します。 攻撃者は、巧妙に細工された HTTP 要求を該当システムに送信することによって、この脆弱性を不正利用する可能性があります。 この不正利用により、攻撃者は任意のシステム ファイルを上書きし、システムを不安定にする可能性があります。

デフォルト設定で実行しているシステムが影響を受けます。

この脆弱性は、Cisco IMC Supervisor については Cisco Bug ID CSCus36435（登録ユーザ専用）、Cisco UCS Director については CSCus62625（登録ユーザ専用）として文書化され、Common Vulnerabilities and Exposures（CVE）ID CVE-2015-6259 が割り当てられています。

脆弱性スコア詳細

シスコは本アドバイザリでの脆弱性に対し、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

CSCus62625/CSCus36435 Cisco IMC Supervisor and Cisco UCS Director Remote File Overwrite 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	Complete	None
CVSS Temporal Score - **6.4**					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

影響

この脆弱性の不正利用が成功するとシステム ファイルが上書きされ、その結果、システムが不安定になったり、DoS 状態が発生したりします。

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 Alerts アーカイブや、後続のアドバイザリを参照して侵害の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、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。

Cisco IMC Supervisor

ソフトウェア バージョン 1.0.0.1 より前のすべてのバージョンが該当します。

ソフトウェア バージョン 1.0.0.0 を実行しているユーザは、システムに 1.0.0.1 以降のパッチを適用する必要があります。 パッチは、次の URL にある Cisco Software Center からダウンロードできます。
https://software.cisco.com/download/release.html?mdfid=286283219&softwareid=286283500&os=&release=1&relind=AVAILABLE&rellifecycle=&reltype=latest&i=!pp

Cisco UCS Director

ソフトウェア バージョン 5.2.0.1 より前のすべてのバージョンが該当します。

ソフトウェア バージョン 5.3.0.0 に修正が含まれています。

5.2.0.1 より前のバージョンを実行しているユーザは、5.2.0.1 以降または 5.3.0.0 以降にアップグレードする必要があります。

5.2.0.0 を実行しているユーザは、5.2.0.1 以降のパッチを適用する必要があります。 パッチは、次の URL にある Cisco Software Center から入手できます。
https://software.cisco.com/download/release.html?mdfid=286283454&flowid=72903&softwareid=285018084&release=5&relind=AVAILABLE&rellifecycle=&reltype=latest

回避策

回避策はありません。

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 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 からソフトウェア パッチおよびバグ フィックスを入手することができます。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、シスコ認定パートナー、リセラー、およびディストリビュータ (認定サードパーティ 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）に連絡してソフトウェア パッチおよびバグ フィックスを入手してください。

- +1 800 553 2447（北米内からのフリー ダイヤル）
- +1 408 526 7209（北米以外からの有料通話）
- E メール：tac@cisco.com

ソフトウェア パッチまたはバグ フィックス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 にソフトウェア パッチまたはバグ フィックスを要求してください。

さまざまな言語向けの各地の電話番号、説明、電子メール アドレスなどの、この他の TAC の連絡先情報については、シスコ ワールドワイドお問い合わせ先（http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html）を参照してください。

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。

この脆弱性はシスコ内部でのセキュリティ テスト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 に掲載されます。

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150902-cimcs

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
- fulldisclosure@seclists.org

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。

今後のドキュメントや関連コンテンツの入手手順については、Security Vulnerability Policy の Receiving Security Vulnerability Information from Cisco を参照してください。

更新履歴

Revision 1.0	2015-September-02	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/web/about/security/psirt/security_vulnerability_policy.html を参照してください。 この Web ページには、Cisco Security Advisory 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。 すべてのシスコ セキュリティ アドバイザリは、http://www.cisco.com/go/psirt/ で確認することができます。

Cisco Security Advisories
Cisco Intrusion Prevention System Signatures
Cisco Applied Mitigation Bulletins
Cisco Security Blog
Cisco Event Response Pages
Cisco IntelliShield Alerts
Cisco Security Notices
Cisco Security Responses
Cisco Cyber Risk Reports
Cisco Security White Papers
Snort Rules