AppManager と SNMP

最近発表された SNMP の脆弱性に関する CERT の勧告に関連してお客様から寄せられた質問に対する回答

2002 年 3 月

この文書では、NetIQ AppManager Suite が SNMP を使用する方法を説明し、最近 CERT が発表した SNMP の脆弱性に関する勧告書によって明らかになった潜在的な問題に対するお客様の疑問に答えます。

目次

はじめに **3**

Q&A **3**

AppManager は SNMP を使用していますか？ 3

SNMP を使用している AppManager のモジュールとコンポーネントは何ですか？ 4

SNMP を「オフ」にした場合、AppManager の使用にはどんな影響が出ますか？ 5

SNMP の脆弱性に関連して NetIQ では何らかのパッチまたは修正プログラムを提供する予定はありますか？ 5

CERT およびさまざまなベンダーが推奨する修正プログラムやパッチが AppManager に何からの影響を及ぼす可能性はありますか？ 5

ご注意

NetIQ Corporation（以下 NetIQ 社といいます）はこの文書を「現状有姿」の状態で提供し、明示的であるか暗黙的であるかを問わず、いかなる種類の保証も行いません。また、NetIQ 社は、商品適合性または特定の目的に対する適合性についてもいっさいの暗黙的保証を行いません。米国内には、特定の取引における明示的または暗黙的保証の免責を認めていない州があります。したがって、このような州では、上記の条項がお客様に適用されないこともあります。

この文書とこの文書に記載されているソフトウェアは、使用許諾契約または機密保持契約に基づいて提供され、当該の契約書の条項に準拠して使用することが許可されます。書面による NetIQ 社の許可なしに、この文書を賃貸、売買、または貸与することは禁止されています。著作権情報を削除しないかぎり、内部的な配布を目的としてこの文書を複写することは許可されています。この文書で使用されている会社名、氏名、およびデータは、特に断らないかぎり架空のもので実在しません。

この文書には、技術的に不正確な記述や誤植が含まれている可能性があります。この文書に記載されている情報には定期的に変更が加えられます。これらの変更は文書の改訂に伴って公開されます。また、NetIQ 社では、この文書に記載されている製品に随時、改善または変更を加えています。

© 1995-2002 NetIQ Corporation, all rights reserved.

U.S. Government Restricted Rights: Use, duplication, or disclosure by the Government is subject to the restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of the DFARs 252.227-7013 and FAR 52.227-29(c) and any successor rules or regulations.

AppManager、AppManager ロゴ、Knowledge Scripts、Work Smarter、NetIQ Partner Network、NetIQ Partner Network ロゴ、Chariot、Pegasus、Qcheck、ADcheck、NetIQ Security Manager、NetIQ File and Storage Administrator、OnePoint、OnePoint ロゴ、OnePoint Directory Administrator、OnePoint Resource Administrator、OnePoint Exchange Administrator、OnePoint Domain Migration Administrator、OnePoint Operations Manager、OnePoint File Administrator、OnePoint Event Manager、Enterprise Administrator、Knowledge Pack、ActiveKnowledge、ActiveAgent、ActiveEngine、Mission Critical Software、Mission Critical Software ロゴ、Ganymede、Ganymede Software、Ganymede ロゴ、NetIQ,、および NetIQ ロゴは、米国およびその他の国や地域における米国 NetIQ Corporation の商標または登録商標です。この文書に記載されているその他の会社名および製品名はあくまでも指摘を目的として使用されており、それらは一般に当該の企業の商標または登録商標です。

はじめに

2 月 12 日火曜日、CERT（Computer Emergency Response Team）は、『Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol（勧告書 CA-2002-03 Simple Network Management Protocol の多くの実装におけるさまざまな脆弱性）』というタイトルで、SNMP のセキュリティ上の脆弱性に関するセキュリティ勧告書を公開しました。この勧告書では、複数のベンダーの SNMP 実装に潜む多数の脆弱性が報告されています。これらの脆弱性は、不正な特権的アクセスやサービスを無効にする攻撃を許可したり、コンピュータの不安定な動作を招く可能性があります。管理対象となるサイトがいずれかのキャパシティで SNMP を使用している場合、CERT/CC では、この勧告書を読み、http://www.cert.org/advisories/CA-2002-03.htmlに投稿されているアドバイスに従うことを推奨しています。

この文書では、Q&A 形式により、AppManager と報告された SNMP の脆弱性に関連してお客様から寄せられたいくつかの疑問に答えます。

Q&A

AppManager は SNMP を使用していますか？

NetIQ AppManager Suite の基本的な機能と情報のやり取りは SNMP サービスに依存していません。AppManager の中核となるコンポーネント（エージェント、管理サーバー、リポジトリ、コンソール、および大部分の監視モジュール）は、SNMP サービスなしに動作することができます。

次の 3 つの AppManager Knowledge Script は、SNMP サービスをインストールしている場合に SNMP サービスと情報をやり取りしますが、その他の SNMP 機能は使用しません。

- General_ServiceDown
- General_ServiceChange
- General_ServiceHung

しかし、いくつかの AppManager 監視モジュールは SNMP サービスの使用に依存して、監視対象となるデバイスからデータを収集したり、SNMP「トラップ」を発生させます。

システムにインストールされている他のアプリケーションと同様、基盤となるオペレーティングシステム内で SNMP の脆弱性が不正に利用された場合、AppManager が何らかの影響を受ける可能性があります。しかし、NetIQ では、AppManager の内部に AppManager 独自の SNMP の脆弱性が含まれているとは認識していません。以下のページでは、特定された脆弱性の問題が解決されるまでの間、多数のユーザが SNMP サービスを無効にすることを

選択したという前提で、AppManager 内での SNMP の使用と、SNMP を無効にした場合に AppManager の操作が被る影響について説明します。

SNMP を使用している AppManager のモジュールとコンポーネントは何ですか？

簡潔に言えば、AppManager の大部分のハードウェア監視モジュールと、サードパーティのシステム管理フレームワークに対応した一部の AppManager「コネクタ」は、SNMP を使用し、SNMP を必要とします。次に、SNMP を使用するモジュールとコネクタの一覧を示します。

モジュール/コネクタ	SNMP に依存する監視機能
AppManager for Compaq Insight Manager（CIM）	大部分の Knowledge Script
AppManager for Dell Open Manager	大部分の Knowledge Script
AppManager for IBM Netfinity Manager	大部分の Knowledge Script
AppManager for HP TopTools	大部分の Knowledge Script
AppManager for Siemens Serverview	大部分の Knowledge Script
AppManager Connector for HP Network Node Manager（NNM）	NNM を使用したすべてのデータ通信は SNMP 経由で行われます。
AppManager Connector for HP VantagePoint Operations（VPO）	VPO を使用したすべてのデータ通信は SNMP 経由で行われます。
AppManager Connector for Aprisma Spectrum	Spectrum を使用したデータ送信は SNMP 経由で行われます。
AppManager Connector to NetIQ End2End	End2End を使用したすべてのデータ通信は SNMP 経由で行われます。

また、いくつかの方式で SNMP サービスを使用したり、SNMP サービスとデータをやり取りする 8 つの Knowledge Script があります。

- General_SNMPGet
- General_SNMPWalk
- Async_SNMPTrap
- NTAdmin_SNMPSet
- NetServices_DHCPHealthCheck
- NetServices_WINSReplication
- NT_NetworkBusy

この文書には、NetIQ の現在の製品計画に基づいた将来の展望が記載されています。したがって、実際の結果が将来の展望と実質的に異なるものになる可能性があることをあらかじめご承知おきください。

- Action_SnmpTrap
- Action_ExtendedSnmpTrap

SNMP を「オフ」にした場合、AppManager の使用にはどんな影響が出ますか？

1 つまたは複数の AppManager コンポーネント（管理エージェント、リポジトリ、または管理サーバー）を実行するサーバーで SNMP サービスをシャットダウンした場合に発生する唯一の問題は、前述のハードウェア監視モジュール、コネクタ、および Knowledge Script がそのサーバーで使用できなくなるということです。もちろん、それ以外の AppManager の機能は従来どおり使用できます。

SNMP の脆弱性に関連して NetIQ では何らかのパッチまたは修正プログラムを提供する予定はありますか？

AppManager が独自の影響を受けることはないため、報告された SNMP の脆弱性に関連して、NetIQ が何らかのパッチまたは修正プログラムを提供する予定はありません。ただし、NetIQ ではお客様に、CERT およびさまざまなベンダーが推奨する修正プログラムまたはパッチの実装を強くお勧めします。

CERT およびさまざまなベンダーが推奨する修正プログラムやパッチが AppManager に何からの影響を及ぼす可能性はありますか？

お客様の側で、一部の監視機能の設定を変更しなければならなくなる可能性があります（たとえば、「コミュニティ文字列」の変更など）。ローカルな SNMP 構成に合わせて AppManager の設定に変更を加える際の指針については、AppManager のマニュアルを参照してください。

この文書には、NetIQ の現在の製品計画に基づいた将来の展望が記載されています。したがって、実際の結果が将来の展望と実質的に異なるものになる可能性があることをあらかじめご承知おきください。