トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ

soft-security
@itg.hitachi.co.jp

2003.07.07更新

DNSリゾルバライブラリに関するセキュリティ問題の説明

2002.06.28に米国CERT/CCからDNSリゾルバ(*)ライブラリに関するセキュリティ問題（Advisory CA-2002-19)が公表されました。
本件，DNSリゾルバライブラリの実装にバッファオーバーフローの問題が確認されたもので，脆弱性を悪用されると、リモートからDNSリゾルバを使用しているアプリケーションの実行権限で任意のコードを実行されたり、DoS(Denial of Service)状態に陥る可能性があります。

*)DNSリゾルバ
DNSサーバにホスト名やIPアドレス情報を問合せするクライアント側のプログラムの総称

弊社ソフトウェア事業部より提供している製品について，本問題の影響がある製品を以下に示します。これらの製品については，対策手順等の情報を提供させていただきます。

■影響がある製品 (情報更新日：2003.05.23)

対策	製品名	適用OS	更新日
HS02-014-01	JP1/Cm2/Extensible SNMP Agent	Linux	2003.05.23
HS02-014-02	JP1/Agent for Process Management	Linux	2002.12.25

更新履歴 ：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にな

らないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

ソフトウェア製品セキュリティ情報
Software Vulnerability Information

ソフトウェア事業部 (Software Division)

2003.07.07更新

HS02-014;

DNSリゾルバライブラリに関するセキュリティ問題の説明

JP1/Cm2/Extensible SNMP Agent DNS Resolver の対策

インターネットのセキュリティに関する調査・報告を行っている米国のCERT/CC(Computer Emergency Response Team Coordination Center)は，「Buffer Overflows in Multiple DNS Resolver Libraries」というAdvisoryを発行しました。ここではDNSリゾルバライブラリの実装においてバッファオーバーフローの問題を報告しています。詳細は，Advisory CA-2002-19を参照願います。

Linux版のJP1/Cm2/Extensible SNMP Agentは，OSが提供するDNSリゾルバライブラリに対するパッチ対策を行なっただけでは，完全に対策できない問題がありました。

１．現象

JP1/Cm2/Extensible SNMP Agentは，環境設定定義ファイルに記述されたトラップあて先やsnmptrapコマンド,systemtrapコマンドの「ノード名」、「agentアドレス」がホスト名の場合に，IPアドレス取得のためにDNSリゾルバライブラリを利用しています。この時に，不正なDNS応答を

トップ
What's New
お知らせ
御参考（警告情報など）
ソフトウェア製品セキュリティ情報
セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

受信すると，該当するシステム上で任意のコードを実行したり，DoS(Denial of Service)状態に陥る危険性があります。

２．該当形名・バージョン，および対策版の提供

各形名の最新バージョンについて対策版をご提供いたします。この対策版へのバージョンアップをお願いします。なお，対策版の提供方法は，JP1/Cm2/Extensible SNMP Agentサポートサービスのご契約の有無によって異なります。

本脆弱性の影響があるJP1/Cm2/Extensible SNMP Agentの形名/バージョン

形名	対象バージョン	適用OS	吸収予定バージョン	提供時期
P-9S42-5A11	05-20	Redhat Linux 5.2 日本語版	05-20-/A	2003.08予定
P-9S42-6A61	06-00 06-00-/A 06-50 06-71	Red Hat Linux 6.1/6.2 日本語版 Red Hat Linux 7.1/7.2 Turbo Linux Server 6.1 日本語版 Red Hat Linux Advanced Server 2.1	06-71-/A	提供済み

（snmptrapコマンド,systemtrapコマンドについては05-20,06-00,06-00/A,06-50がこの問題に該当します。06-71はこの問題に該当しません）

- サポートサービスをご契約されているお客様

  サポートサービスの改良版の提供についてのホームページをご参照いただき，ホームページでご案内している手順にしたがって，対策版を

ご入手ください。

- サポートサービスをご契約されていないお客様

  JP1/Cm2/Extensible SNMP Agentに関しては，ライセンス管理を適切に行なう必要があるため，お手数ですが，こちら より提供をご依頼ください。

- 回避策

  この脆弱性に対しては，運用での下記回避策があります。対策版が発行されるまではこの回避策を実施して下さい。

  （1）/etc/SnmpAgent.d/snmpd.confのtrap-dest:ラベルにホスト名を指定している場合は以下の回避策を実施下さい。

  a. /etc/SnmpAgent.d/snmpd.confファイルをエディタで開きます。

     trap-dest:ラベルの後ろに記述されているホスト名をIPアドレスに変更します。

     (例)

     変更前 trap-dest: host-1

     変更後 trap-dest: 15.2.113.223

  b. 上記定義ファイルの変更内容を有効にするために JP1/Cm2/Extensible SNMP Agentを再起動します。

     以下のコマンドをスーパーユーザで実行します。

     /opt/CM2/ESA/bin/snmpstart

（2）snmptrapコマンド,systemtrapコマンドを使用している場合で、コマンドの引数に指定する「ノード名」、「agentアドレス」にホスト名を指定している場合は以下の回避策を実施下さい。
（05-20,06-00,06-00/A,06-50がこの問題に該当します。06-71はこの問題に該当しません）

a. snmptrapコマンドの場合

snmptrapコマンドの引数に指定する「ノード名」、「agentアドレス」をホスト名からIPアドレスに変更します。

(例)ノード名：host-1，agentアドレス：host-2の場合

変更前 snmptrap host-1 "" host-2 6 100 ""

変更後 snmptrap 15.2.113.223 "" 15.2.113.225 6 100 ""

b. systemtrapコマンドの場合

systemtrapコマンドの引数に指定する「ノード名」、「agentアドレス」をホスト名からIPアドレスに変更します。

(例)ノード名：host-1，agentアドレス：host-2の場合

変更前 systemtrap -s host-1 host-2 program1 Cri

変更後 systemtrap -s 15.2.113.223 15.2.113.225 program1 Cri

更新履歴 ：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

- 弊社では，セキュリティ対応に関して正確な情報を提供するよう努力しておりますが，セキュリティ問題に関する情報は変化しており，当ホームページで記載している内容を予告なく変更することがありますので，あらかじめご了承ください。情報ご参照の際には，常に最新の情報をご確認いただくようお願いします。
- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ

ソフトウェア製品セキュリティ情報
Software Vulnerability Information

ソフトウェア事業部 (Software Division)

トップ

What's New

お知らせ

御参考（警告情報など）

ソフトウェア製品セキュリティ情報

セキュリティ対応機関へのリンク

お問い合わせ
soft-security
@itg.hitachi.co.jp

2003.07.07更新

HS02-014;

DNSリゾルバライブラリに関するセキュリティ問題の説明

JP1/Agent for Process Management DNS Resolver の対策

インターネットのセキュリティに関する調査・報告を行っている米国のCERT/CC(Computer Emergency Response Team Coordination Center)は，「Buffer Overflows in Multiple DNS Resolver Libraries」というAdvisoryを発行しました。ここではDNSリゾルバライブラリの実装においてバッファオーバーフローの問題を報告しています。詳細は，Advisory CA-2002-19を参照願います。

Linux版のJP1/Agent for Process Managementは，OSが提供するDNSリゾルバライブラリに対するパッチ対策を行なっただけでは，完全に対策できない問題がありました。

１．現象

JP1/Agent for Process Managementは，定義ファイルに記述されたイベント宛て先や発信元アドレスがホスト名の場合に，IPアドレス取得のために

DNSリゾルバライブラリを利用しています。この時に，不正なDNS応答を受信すると，該当するシステム上で任意のコードを実行したり，DoS(Denial of Service)状態に陥る危険性があります。

２．該当形名・バージョン，および対策版の提供

各バージョン向けの対策版をご提供いたします。なお，対策版の提供方法は，JP1/Agent for Process Managementサポートサービスのご契約の有無によって異なります。

本脆弱性の影響があるJP1/Agent for Process Managementの形名/バージョン

形名	対象バージョン	適用OS	吸収予定バージョン	提供時期
P-9S42-5J11	05-21	Redhat Linux 5.2 日本語版	05-21-/A	提供済み
P-9S42-6J61	06-71-/A 06-71	Red Hat Linux 6.1/6.2 日本語版 Red Hat Linux 7.1/7.2 Turbo Linux Server 6.1 日本語版 Red Hat Linux Advanced Server 2.1	06-71-/B	
	06-51-/B 06-51-/A 06-51	Red Hat Linux 6.1/6.2 日本語版 Red Hat Linux 7.1/7.2 Turbo Linux Server 6.1 日本語版	06-51-/C	
		Red Hat Linux 5.2 日本語版		

	06-00-/B 06-00-/A 06-00	Red Hat Linux 6.1/6.2 Turbo Linux Server 6.1 日本語版	06-00-/C	

- サポートサービスをご契約されているお客様

  サポートサービスの改良版の提供についてのホームページをご参照いただき，ホームページでご案内している手順にしたがって，対策版をご入手ください。

- サポートサービスをご契約されていないお客様

  JP1/Agent for Process Managementに関しては，ライセンス管理を適切に行なう必要があるため，お手数ですが，こちら より提供をご依頼ください。

- 回避策

  この脆弱性に対しては，運用での下記回避策がありますが速やかに対策版の入手をお勧めします。

  定義ファイルのイベント宛て先や発信元アドレスをホスト名ではなく，IPアドレスで記述すれば，本問題を回避することができます。

  （1）宛て先定義ファイルの宛て先は，ホスト名ではなくIPアドレスで記述します。

  1)対象ファイル

  ・SNMPエージェント環境設定ファイル

  (/etc/SnmpAgent.d/snmpd.conf)

  ・起動イベント宛て先定義ファイル

  (/etc/opt/CM2/APM/conf/apmdest.conf)

  ・JP1/Cm2/Internet SNMP Gateway宛て先定義ファイル

  (/etc/opt/CM2/APM/conf/apmproxy.conf)

  2)変更方法

①SNMPエージェント環境設定ファイル

トラップの宛て先(trap-dest:ラベルの後ろ)にホスト名が記述されている場合，IPアドレスに変更します。

(例)

trap-dest: host-1 ⇒ trap-dest: 15.2.113.223

②起動イベント宛て先定義ファイル

イベントの宛て先がホスト名で記述されている場合，IPアドレスに変更します。

③JP1/Cm2/Internet SNMP Gateway宛て先定義ファイル

JP1/Cm2/Internet SNMP Gateway及び，監視マネージャの宛て先がホスト名で記述されている場合，IPアドレスに変更します。

(例)

{host-isg;host-sso1;host-sso2;} ⇒

{100.100.100.1;100.100.100.2;100.100.100.3;}

（2）イベント通知発行元アドレス定義ファイルに発行元アドレスをIPアドレスで記述します。

1)対象ファイル

・イベント通知発行元アドレス定義ファイル

(/etc/opt/CM2/APM/conf/apmaddr.conf)

2)変更方法

①稼動中のJP1/Agent for Process Managementのバージョンを確認します。

対象のファイルは，バージョン06-51以降に提供された為，稼動中のJP1/Agent for Process Managementがそれ以前の場合，対象ファイルを新規に作成し②にしたがって発行元アドレスをIPアドレスを記載してください。

②イベント発行元アドレスが未記入の場合、任意のIPアドレスを指定します。

イベントの発行元にするIPアドレスと「；(セミコロン)」を記述する。この場合，JP1/Server System Observerが認識するアドレスにしなければなりません。

(例)

1.1.255.1;

（3）上記定義ファイルの変更内容を有効にするためにJP1/Agent for Process Managementを再起動します。

1)再起動方法

①JP1/Agent for Process Managementを停止します。

/opt/CM2/APM/bin/apmstopコマンドを実行します。

②JP1/Agent for Process Managementを起動します。

/opt/CM2/APM/bin/apmstartコマンドを実行します。

③JP1/Agent for Process Managementが正常起動したことを確認します。

psコマンドでプロセス(hiapmmib,apmProcMng)が存在すること。及び，ログファイル(/var/opt/CM2/APM/log/apmerr.log)にエラーメッセージがないことを確認します。

更新履歴 ：

- 2003.07.07 : このセキュリティ情報ページをリニューアルしました。

- 当ホームページに記載されている製品には，他社開発製品が含まれております。これらのセキュリティ情報については他社から提供，または公開された情報を基にしております。弊社では，情報の正確性および完全性について注意を払っておりますが，開発元の状況変化に伴い，当ホームページの記載内容に変更が生じることがあります。
- 当ホームページはセキュリティ情報の提供を目的としたものであり，法律上の責任を負うものではありません。お客様が独自に行なった(あるいは行なわなかった)セキュリティ対応その他のご行為の結果につきまして，弊社では責任を負いかねます。
- 当ホームページから他サイトのページへのリンクアドレスは情報発信時のものです。他サイトでの変更などを発見した場合には、リンク切れ等にならないように努力はいたしますが、永続的にリンク先を保証するものではありません。

ページトップへ