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

Apache Web Serverに関するセキュリティ問題の説明

2002.06.07に米国CERT/CCからApache Web Serverに関するセキュリティ問題（Advisory CA-2002-17)が公表されました。
本件，Apache Web Serverのチャンク形式データ処理において，リモートから悪用可能な脆弱性があることが確認されたもので，この脆弱性を悪用すると，リモートから任意のコマンドを実行したり，DoS攻撃に悪用できてしまう可能性があります。

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：2002.09.30)

対策	製品名	適用OS	更新日
HS02-008-01	JP1/Cm2/Network Node Manager	HP-UX，Solaris	2002.09.30
HS02-008-02	Hitachi Web Server	HP-UX，Solaris，AIX，Linux	2002.06.28

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

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

HS02-008;

Apache Web Serverに関するセキュリティ問題の説明

JP1/Cm2/Network Node Manager 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，「Apache Web Server Chunk Handling Vulnerability」というAdvisoryを発行しました。ここでは，Apache Web Serverのチャンク形式データ処理において，リモートから悪用可能な脆弱性があるという問題を報告しています。詳細は，Advisory CA-2002-17を参照願います。

JP1/Cm2/Network Node Managerに含まれる Webサーバにおいても同様の脆弱性があります。

１．現象

チャンク形式の不当なリクエストを受信した場合に，JP1/Cm2/Network Node Manager の Webサーバプロセスがセグメンテーションフォルトで異常終了することがあります。Webサーバプロセスが異常終了した場合は，制

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
個人情報保護ポリシーにご同意頂ける場合のみ、上記アドレスをご利用下さい。ご同意頂けない場合には、お問い合わせに回答できない場合があります。
なお、入力頂いた個人情報は本ポリシーに従って適切に管理し、問合せ対応のためにのみ使用します。第三者への個人情報の提供、預託、開示は法令に基づく場合を除いて行いません。
お問い合わせへの回答後、個人情報は当社が責任を持って適切に廃棄いたします。
日立および他社の商品名称に関する記述

御プロセスにより新たなサーバプロセスが起動されますが，このとき，コアダンプの出力とサーバプロセス再起動による負荷が掛かります。悪意の第三者によりこの不当なリクエストが連続的に送信されると，DoS(Denial of Service,サービス使用不可)攻撃になる危険性があります。

２．該当形名・バージョン，および対策パッチの提供

各プラットフォーム・各バージョン向けの対策パッチをご提供いたします。

３．その他

下記以外の他のバージョンについては，現在影響有無を調査中です。

本脆弱性の影響があるJP1/Cm2/Network Node Managerの形名/バージョン

形名	対象バージョン	適用OS	対策パッチ		吸収予定バージョン	更新日
			適用手順	ダウンロード		
P-1B42-6161 P-1B42-6261	06-71	HP-UX	HS02-008-01-a	P-1B42-6161_0671SA.tar (890,880byte)	06-71-/A	2002.08.22
P-9D42-6161 P-9D42-6261	06-71	Solaris	HS02-008-01-b	P-9D42-6161_0671SA.tar (587,776byte)	06-71-/A	2002.08.22
P-1B42-6161 P-1B42-6261	06-51	HP-UX	HS02-008-01-c	P-1B42-6161_0651SC.tar (890,880byte)	06-51-/A	2002.08.22
P-9D42-6161 P-9D42-6261	06-51	Solaris	HS02-008-01-d	P-9D42-6161_0651SC.tar (587,776byte)	06-51-/A	2002.08.22
P-1B42-6161 P-1B42-6261	06-50～06-50-/A	HP-UX	HS02-008-01-e	P-1B42-6161_0650SK.tar (890,880byte)	06-50-/B	2002.09.30
P-9D42-6161 P-9D42-6261	06-50～06-50-/A	Solaris	HS02-008-01-f	P-9D42-6161_0650SB.tar (587,776byte)	06-50-/B	2002.09.30
P-1B42-6161 P-1B42-6261	06-00～06-00-/A	HP-UX	HS02-008-01-g	P-1B42-6161_0600SF.tar (890,880byte)	06-00-/B	2002.09.30
P-9D42-6161 P-9D42-6261	06-00～06-00-/C	Solaris	HS02-008-01-h	P-9D42-6161_0600SC.tar (587,776byte)	06-00-/D	2002.09.30

※本対策パッチには，前提となる関連パッチはありません。

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。
- 2002.09.30 : バージョン 06-50, 06-00 のセキュリティ問題対策パッチの提供を開始しました。

- 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

HS02-008;

Apache Web Serverに関するセキュリティ問題の説明

Hitachi Web Server 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，「Apache Web Server Chunk Handling Vulnerability」というAdvisoryを発行しました。ここでは，Apache Web Serverのチャンク形式データ処理において，リモートから悪用可能な脆弱性があるという問題を報告しています。詳細は，Advisory CA-2002-17を参照願います。

Hitachi Web Serverにおいてもこの脆弱性があります。

１．現象

チャンク形式の不当なリクエストを受信した場合に，Hitachi Web Serverのサーバプロセスがセグメンテーションフォルトで異常終了することがあります。サーバプロセスが異常終了した場合は，制御プロセスにより新たなサーバプロセスが起動されますが，このとき，コアダンプの出力とサー

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

バプロセス再起動による負荷が掛かります。悪意の第三者によりこの不当なリクエストが連続的に送信されると，DoS(Denial of Service,サービス使用不可)攻撃になる危険性があります。

２．該当形名・バージョン，および対策パッチの提供

各プラットフォーム・各バージョン向けの対策パッチをご提供いたします。なお，対策パッチの提供方法は，Hitachi Web Serverサポートサービスのご契約の有無によって異なります。

[ご注意]

この脆弱性に対しては，運用での回避策はありません。必ず，下記手順にしたがって対策パッチを適用いただくよう，お願いいたします。

- Hitachi Web Serverサポートサービスをご契約されているお客様
  Hitachi Web Serverサポートサービス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，対策パッチをご入手ください。
- Hitachi Web Serverサポートサービスをご契約されていないお客様
  Hitachi Web Server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。

本脆弱性の影響があるHitachi Web Serverの形名/バージョン

製品名	形名	Ver-Rev	対応OS
	P-1B41-E111	01-02-/A 01-02 01-01-/A 01-01 01-00-/A 01-00	HP-UX10.20
	P-1B41-E121	01-02-/A 01-02 01-01-/A	HP-UX11.0/11i

Hitachi Web Server	P-1B41-E121B1	01-01 01-00-/A 01-00	
	P-1M41-E111	01-02 01-01	AIX5L V5.1
	P-1L41-E111	01-01	Turbolinux Server 6 for MP Series
	P-9D41-E111	01-02 01-01 01-00-/A 01-00	Solaris2.6/7/8
	P-9S41-E111	01-01-/A 01-01	Turbo Linux日本語版 6.1, RedHat Linux 6.2 日本語版

下記のCosminexus Server製品に同梱のHitachi Web Serverについても，該当します。

Cosminexus製品名	形名	対応OS
Cosminexus Server - Web Edition	P-1BZ4-1S31	HP-UX11.0/11i
	P-9DZ4-1D31	Solaris2.6/7
Cosminexus Server - Standard Edition	P-1BZ4-1T31	HP-UX11.0/11i
	P-9DZ4-1E31	Solaris2.6/7
Cosminexus Server - Enterprise Edition	P-1BZ4-1U31	HP-UX11.0/11i
	P-9DZ4-1F31	Solaris2.6/7
Cosminexus Server - Web Edition Version 4	P-1BZ4-1S41	HP-UX11.0/11i
	P-9DZ4-1D41	Solaris7/8
Cosminexus Server - Standard Edition Version 4	P-1BZ4-1T41	HP-UX11.0/11i
	P-9DZ4-1E41	Solaris7/8
	P-1MZ4-1E41	AIX5L V5.1

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