

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)

ホーム | 製品&サービス | >> セキュリティ |

英語ページへ

HITACHI
Inspire the Next

日立サイトの検索 by Google

> GO

> 詳細な検索

ホーム > 製品セキュリティ情報 > ソフトウェア事業部セキュリティ情報 > HS05-023

2005.10.31更新

Groupmax CollaborationおよびCosminexus Collaborationにおけるクロスサイトスクリプティング問題およびDoSの脆弱性

■ 影響がある製品

対策	製品名	適用OS	更新日
HS05-023-01	Groupmax Collaboration Portal, Groupmax Collaboration Web Client - Forum/File Sharing, Cosminexus Collaboration Portal, Cosminexus Collaboration Portal - Forum/File Sharing	Windows	2005.10.31

■ 問題の説明

上記の製品において、クロスサイトスクリプティング問題及びDoSの脆弱性が存在することが判明しました。

例えば、悪意を持った第三者から不正なスクリプトを実行させられ

> 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](mailto:soft-security@itg.hitachi.co.jp)

[@itg.hitachi.co.jp](mailto: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

る可能性があります。またこの脆弱性を利用した悪意のある第三者からの攻撃により、上記の製品がサービス不能に陥る可能性があります。



更新履歴：

- 2005.10.31 : このセキュリティ情報ページを新規作成および発信しました。

-
- 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に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いたします。
 - 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。

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)

| ホーム | 製品&サービス | >> セキュリティ |

» 英語ページへ

日立サイトの検索 by Google

> GO

> 詳細な検索

ホーム > 製品セキュリティ情報 > ソフトウェア事業部セキュリティ情報 > HS05-023-01

2005.10.31更新

HS05-023;

Groupmax CollaborationおよびCosminexus Collaborationにおけるクロスサイトスクリプティング問題およびDoSの脆弱性

Groupmax CollaborationおよびCosminexus Collaborationの 対策

Groupmax CollaborationおよびCosminexus Collaborationの構成製品である

Collaboration - ScheduleとCollaboration - Calendarにおいて、クロスサイトスクリプティング問題およびDoSの脆弱性があります。

- クロスサイトスクリプティング問題

Collaboration - Scheduleまたは、Collaboration - Calendarに不正なスクリプトを送信した場合、表示された画面でスクリプトが実行される場合があります。

- DoSの脆弱性

Collaboration - Scheduleに対して不正なリクエストの送信を繰り返すことにより、リクエストを受け付けなくなる場合があります。

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

> 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](mailto:soft-security@itg.hitachi.co.jp)[@itg.hitachi.co.jp](mailto: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

バージョンアップ、またはリビジョンアップをお願いします。



[該当形名・バージョン, および対策版の提供]

セット製品名	形名	対象バージョン	適用OS	吸収バージョン	提供時期	更新日
Groupmax Collaboration Portal	P-2646-6354	07-00~ 07-10-/B	Windows	07-10-/C	2005.10.31	2005.10.31
Cosminexus Collaboration Portal	P-2443-3D64	06-00~ 06-10-/B		06-10-/C	2005.10.31	2005.10.31
Groupmax Collaboration Web Client - Forum/File Sharing	P-2746-E354	07-00~ 07-10-/A		07-10-/B	2005.10.31	2005.10.31
Cosminexus Collaboration Portal - Forum/File Sharing	P-2443-3E64	06-00~ 06-10-/A		06-10-/B	2005.10.31	2005.10.31

[構成製品の該当形名]

セット商品名		対象となる構成製品		
製品名	形名	形名	構成製品名	適用OS
Groupmax Collaboration Portal	P-2646-6354	CLB1-CBBW	Collaboration - Bulletin board	
		CLB1-CCCW	Collaboration - Calendar	
		CLB1-CCUW	Collaboration - Common Utility	
		CLB1-CDAW	Collaboration - Directory Access	
		CLB1-CFRW	Collaboration - Forum	
		CLB1-CFSW	Collaboration - File Sharing	
		CLB1-CMLW	Collaboration - Mail	
		CLB1-CNVW	Collaboration - Navigation View	
CLB1-COCW	Collaboration - Online Community Management			

		CLB1-CSCW	Collaboration - Schedule
		P-2443-3464&UWN	Cosminexus Portal Framework - Light
		P-2446-5W54	Groupmax Collaboration - Directory Converter
Cosminexus Collaboration Portal	P-2443-3D64	CLB1-CBBW	Collaboration - Bulletin board
		CLB1-CCCW	Collaboration - Calendar
		CLB1-CCUW	Collaboration - Common Utility
		CLB1-CDAW	Collaboration - Directory Access
		CLB1-CFRW	Collaboration - Forum
		CLB1-CFSW	Collaboration - File Sharing
		CLB1-CMLW	Collaboration - Mail
		CLB1-CNVW	Collaboration - Navigation View
		CLB1-COCW	Collaboration - Online Community Management
		CLB1-CSCW	Collaboration - Schedule
		P-2443-3464&UWN	Cosminexus Portal Framework - Light
P-2446-5W54	Groupmax Collaboration - Directory Converter		
Groupmax Collaboration Web Client - Forum/File Sharing	P-2746-E354	CLB1-CBBW	Collaboration - Bulletin board
		CLB1-CCCW	Collaboration - Calendar
		CLB1-CCUW	Collaboration - Common Utility
		CLB1-CDAW	Collaboration - Directory Access
		CLB1-CFRW	Collaboration - Forum
		CLB1-CFSW	Collaboration - File Sharing
		CLB1-CNVW	Collaboration - Navigation View
		CLB1-COCW	Collaboration - Online Community Management
		P-2443-3464&UWN	Cosminexus Portal Framework - Light
		P-2446-5W54	Groupmax Collaboration - Directory Converter
		CLB1-CBBW	Collaboration - Bulletin board
		CLB1-CCCW	Collaboration - Calendar

Windows

Cosminexus Collaboration Portal - Forum/File Sharing	P-2443-3E64	CLB1-CCUW	Collaboration - Common Utility
		CLB1-CDAW	Collaboration - Directory Access
		CLB1-CFRW	Collaboration - Forum
		CLB1-CFSW	Collaboration - File Sharing
		CLB1-CNVW	Collaboration - Navigation View
		CLB1-COCW	Collaboration - Online Community Management
		P-2443-3464&UWN	Cosminexus Portal Framework - Light
		P-2446-5W54	Groupmax Collaboration - Directory Converter

- 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

Groupmax CollaborationおよびCosminexus Collaboration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。

更新履歴：

- 2005.10.31：Groupmax CollaborationおよびCosminexus Collaborationにおけるクロスサイトスクリプティング問題およびDoSの脆弱性の情報を公開しました。

- 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に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いたします。
- 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](#)