

Software Vulnerability Information

Software Division

HITACHI
Inspire the Next

[Home](#) |
 [Software](#) |
 [Security](#)

[Japanese](#)

Search in the Hitachi site by Google

GO

> Advanced search

[Home](#) >
 [Vulnerability Information](#) >
 [Software Vulnerability Information](#) >
 HS06-014

> TOP

> What's New

> Notifications

> Alert

> Software Vulnerability Information

> Links to Security Organizations

> Email
soft-security@itg.hitachi.co.jp

Before sending an email, you need to read [Privacy Notice](#) and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in [Privacy Notice](#). Only send an email to this address if you are willing to give your consent upon carefully reading [Privacy Notice](#).

Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

> Product names of Hitachi and other manufacturers

Update: July 5, 2006

Cross-site Scripting Vulnerabilities in Groupmax Collaboration Portal and uCosminexus Collaboration Portal

- Affected product

| Corrective actions | Product name | Platform | Last update |
|-----------------------------|---|----------|--------------|
| HS06-014-01 | Groupmax Collaboration Portal, Groupmax Collaboration Web Client - Forum/File Sharing, uCosminexus Collaboration Portal, uCosminexus Collaboration Portal - Forum/File Sharing | Windows | July 5, 2006 |

- Problem description

Cross-site scripting vulnerabilities were found in the above products. Remote users can exploit these vulnerabilities and execute malicious scripts.

Revision history

- July 5, 2006: This page is released.

- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
- The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
- The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in connection with the security countermeasures or other actions that you will take



or have taken (or not taken) by yourself.

- The links to other web sites are valid at the time of the release of the page.
Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

 [Page Top](#)

Software Vulnerability Information

Software Division

HITACHI
Inspire the Next

[Home](#) |
 [Software](#) |
 [» Security](#) |

» Japanese

Search in the Hitachi site by Google

> GO

> Advanced search

Home > Vulnerability Information > Software Vulnerability Information > HS06-014-01

Update: July 5, 2006

HS06-014;

Cross-site Scripting Vulnerabilities in Groupmax Collaboration Portal and uCosminexus Collaboration Portal

Solution for Groupmax Collaboration Portal and uCosminexus Collaboration Portal

Cross-site scripting vulnerabilities were found in Collaboration - File Sharing, which is a component product of Groupmax Collaboration Portal, Groupmax Collaboration Web Client - Forum/File Sharing, uCosminexus Collaboration Portal, and uCosminexus Collaboration Portal - Forum/File Sharing. The fixed versions that are available for recent versions are indicated below. Please upgrade the Groupmax and uCosminexus versions in your system to the appropriate version.

[Affected models and versions]

| Product name | Model | Version | Platform | Fixed version | Release time | Last update |
|--|-------------|-------------------|----------|---------------|---------------|--------------|
| Groupmax Collaboration Portal | P-2646-6354 | 07-20 to 07-20-/C | Windows | 07-20-/D | June 20, 2006 | July 5, 2006 |
| Groupmax Collaboration Web Client - Forum/File Sharing | P-2746-E354 | 07-20 to 07-20-/B | | 07-20-/C | June 20, 2006 | July 5, 2006 |
| uCosminexus Collaboration Portal | P-2443-3D74 | 06-20 to 06-20-/C | | 06-20-/D | June 20, 2006 | July 5, 2006 |
| uCosminexus Collaboration Portal - Forum/File Sharing | P-2443-3E74 | 06-20 to 06-20-/B | | 06-20-/C | June 20, 2006 | July 5, 2006 |

[Component products of affected models]

| Product set | | Affected component | | |
|------------------|-------|--------------------|--------------------------------|----------|
| Product set name | Model | Model | Component name | Platform |
| | | CLB1-CBBW | Collaboration - Bulletin board | |
| | | CLB1-CCCW | Collaboration - Calendar | |
| | | CLB1- | Collaboration - Common | |

> TOP

∨ What's New

> Notifications

> Alert

> Software Vulnerability Information

> Links to Security Organizations

> Email
soft-security@itg.hitachi.co.jp

Before sending an email, you need to read [Privacy Notice](#) and to give your consent to the contents. If you do not give your consent, you may not be able to utilize the services prescribed under the purposes of use in [Privacy Notice](#). Only send an email to this address if you are willing to give your consent upon carefully reading [Privacy Notice](#).

Note that personal information that is sent to this address will be erased as soon as the response to your inquiry is given, and that the Company will not retain the personal information.

> Product names of Hitachi and other manufacturers



| | | | |
|--|-------------|-------------|--|
| Groupmax Collaboration Portal | P-2646-6354 | CCUW | 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-2443-7464 | uCosminexus 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-2443-7464 | uCosminexus Portal Framework - Light |
| | | P-2446-5W54 | Groupmax Collaboration - Directory Converter |
| uCosminexus Collaboration Portal | P-2443-3D74 | 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 |

Windows

| | | | |
|---|-------------|-------------|--|
| uCosminexus Collaboration Portal - Forum/File Sharing | P-2443-3E74 | CLB1-COCW | Collaboration - Online Community Management |
| | | CLB1-CSCW | Collaboration - Schedule |
| | | P-2443-7464 | uCosminexus Portal Framework - Light |
| | | P-2446-5W54 | Groupmax Collaboration - Directory Converter |
| | | 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-2443-7464 | uCosminexus Portal Framework - Light |
| | | P-2446-5W54 | Groupmax Collaboration - Directory Converter |

For details on the fixed versions, contact your Hitachi support service representative.

Revision history

- July 5, 2006: Information about cross-site scripting vulnerabilities in Groupmax Collaboration Portal and uCosminexus Collaboration Portal is released.

-
- Hitachi, Ltd. (hereinafter referred to as "Hitachi") tries to provide accurate information about security countermeasures. However, since information about security problems constantly changes, the contents of these Web pages are subject to change without prior notice. When referencing information, please confirm that you are referencing the latest information.
 - The Web pages include information about products that are developed by non-Hitachi software developers. Vulnerability information about those products is based on the information provided or disclosed by those developers. Although Hitachi is careful about the accuracy and completeness of this information, the contents of the Web pages may change depending on the changes made by the developers.
 - The Web pages are intended to provide vulnerability information only, and Hitachi shall not have any legal responsibility for the information contained in them. Hitachi shall not be liable for any consequences arising out of or in

connection with the security countermeasures or other actions that you will take or have taken (or not taken) by yourself.

- The links to other web sites are valid at the time of the release of the page. Although Hitachi makes an effort to maintain the links, Hitachi cannot guarantee their permanent availability.

 [Page Top](#)