

[NT] DeskNow Mail and Collaboration Server Directory Traversal Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0014.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/03/05

To: list@securiteam.com

Date: 3 Feb 2005 11:27:32 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

DeskNow Mail and Collaboration Server Directory Traversal Vulnerabilities

SUMMARY

<<http://www.desknow.com/desknowmc/index.html>> DeskNow Mail and Collaboration Server is "a full-featured and integrated mail and instant messaging server, with webmail, secure instant messaging, document repository, shared calendars, address books, message boards, web-publishing, anti-spam features, Palm and PocketPC access and much more".

A directory traversal vulnerability was found in DeskNow webmail file attachment upload feature that may be exploited to upload files to arbitrary locations on the server. A malicious webmail user may upload a JSP file to the script directory of the server, and executing it by requesting the URL of the upload JSP file. A second directory traversal vulnerability exists in the document repository file delete feature. This vulnerability may be exploited to delete arbitrary files on the server.

DETAILS

Vulnerable Systems:

* DeskNow Mail and Collaboration Server version 2.5.12 and prior

Securiteam: [NT] DeskNow Mail and Collaboration Server Directory Traversal Vulnerabilities

Immune Systems:

* DeskNow Mail and Collaboration Server version 2.5.14 or newer

On the Windows platform, the default installation of DeskNow Mail and Collaboration Server runs its webmail service using Tomcat Application Server with LOCAL SYSTEM privilege. This advisory documents two directory traversal vulnerabilities that may be exploited by a malicious webmail user to upload/delete files to/from arbitrary directories.

1. Insufficient input sanitization in attachment.do allows file upload to arbitrary directories

DeskNow's webmail allows a logon mail user to upload file attachments when composing an email. Lack of sanitization of the AttachmentsKey parameter allows the user to upload files to arbitrary location on the server. More specifically, It is possible to use directory traversal characters to cause the uploaded file attachment to be saved outside the temporary directory. This may be exploited by a malicious webmail user to upload JSP files to the script execution directory of the server. After uploading the JSP file, it is possible to execute that file by directly requesting it's URL (i.e. [http://\[hostname\]/desknow/jsp/test/poc.jsp](http://[hostname]/desknow/jsp/test/poc.jsp)). Successful exploitation will allow upload and execution of arbitrary JSP code with LOCAL SYSTEM privilege. e.g. a malicious user may upload a JSP file that gives him/her a reverse shell.

2. Insufficient input sanitization in file.do allows deleting of arbitrary files

DeskNow's document repository feature allows a user to store files on the server via the web interface. A user is allowed to delete his/her own files. When the user selects his own file to be deleted, the file name is sent using the select_file parameter as a POST request to file.do. It is possible to use directory traversal characters within this parameter to delete files that do not belong to the user.

Solution:

Upgrade to DeskNow Mail and Collaboration Server Version 2.5.14 or later.

Disclosure Timeline:

23 Jan 05 – Vulnerability Discovered
24 Jan 05 – Initial Vendor Notification
24 Jan 05 – Initial Vendor Reply
25 Jan 05 – Vendor Released Version 2.5.13
25 Jan 05 – Informed Vendor that Vulnerability is not Fully Fixed
27 Jan 05 – Vendor Released Fixed Version 2.5.14
02 Feb 05 – Public Release

ADDITIONAL INFORMATION

The information has been provided by <<mailto:chewkeong@security.org.sg>>

Tan Chew Keong.

The original article can be found at:

<<http://www.security.org.sg/vuln/desknow2512.html>>

Securiteam: [NT] DeskNow Mail and Collaboration Server Directory Traversal Vulnerabilities

<http://www.security.org.sg/vuln/desknow2512.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.