

# [NEWS] Clear Text Password Vulnerability Found in DeskNow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0007.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 04/06/03

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 6 Apr 2003 16:25:58 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Clear Text Password Vulnerability Found in DeskNow

---

## SUMMARY

DeskNow is "an easy-to-use and affordable communication server that can handle all the communication and collaboration needs of your company".

When a user logs into the Web Mail, the username and password is sent in clear text.

## DETAILS

Vulnerable versions:  
DeskNow Version 1.2

When logging in on the Web Mail part the password is sent in clear text. This vulnerability is quit easy to exploit if you are on the same network as the user that logs on this service.

Proof of Concept:  
LOGIN PAGE:

Securiteam: [NEWS] Clear Text Password Vulnerability Found in DeskNow

Here is the capture of the first line of defense from the DeskNow Web Mail

```
OST /desknow/home.do?Action=Login HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,
Referer: http://index.html
Accept-Language: da
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: 192.168.1.27
Content-Length: 67
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: JSESSIONID=31726ABD7F50019824E8DFFBDBCE5627; username=matrix

username=matrix&password=ThisIsMyPassword2&submit=Login&cbremember=checkbox
TTP/1.1 200 OK
Content-Type: text/html; charset=ISO-8859-1
Date: Tue, 25 Feb 2003 16:12:18 GMT
Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
Transfer-Encoding: chunked
Set-Cookie: JSESSIONID=A660DFCFEABBC6899DE5A5F4F6862BBE; Path=/desknow
```

Detection:  
DeskNow Version 1.2 is vulnerable to this attack. Earlier versions may be susceptible as well. To determine if a specific implementation is vulnerable, experiment by following the above transcript.

Workaround:  
None at this time (use HTTPS).

Vendor status:  
Vendor contacted and responded the following:  
"Hi,  
thanks for analyzing our software!  
We are of course well aware of the fact that the password is sent in clear text when using the http protocol.  
Users and administrators can login to DeskNow using the HTTPS protocol for maximum security with data encryption.  
DeskNow supports SSL 3.0 with 128 bit RC4 encryption .  
Regards,  
Dario"

ADDITIONAL INFORMATION

The vulnerability was discovered by <<mailto:der@infowarfare.dk>> Dennis Rand.

=====

Securiteam: [NEWS] Clear Text Password Vulnerability Found in DeskNow

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](mailto:list-unsubscribe@securiteam.com)

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