

Re: Vulnerability in Helpdesk software Hesk 0.92

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-08/0428.html>

From: Thomas Krüger (*krueger_at_k-dns.de*)

Date: 08/30/05

Date: Tue, 30 Aug 2005 15:00:54 +0200

To: s2b@hotmail.com

s2b@hotmail.com schrieb:

>By The Name Of Allah

>

>Vulnerability in Helpdesk software Hesk ..

>

>Vulnerability Type : Login into The Administrator Menu With out Password

>

>Injected version : Helpdesk software Hesk 0.92

>

>Vulnerability Example

>

><http://www.springporttwppd.com/helpdesk/>

>

>add : admin.php

>

><http://www.springporttwppd.com/helpdesk/admin.php>

>

>Choose the username : administrator

>

>Put any password in the password field

>

>change the url to : admin_main.php

>

>http://www.springporttwppd.com/helpdesk/admin_main.php

>

>You Are Noe in the Administrator menu ..

>

>

Hi s2b,

sorry, but I can't confirm that. I can't get any access following your instructions.

The given site uses Basic HTTP Authentication. Requests with this authentication do not depend on the other. There is just the

SecurityFocus Bugtraq: Re: Vulnerability in Helpdesk software Hesk 0.92

Authentication header added.

Even manual alteration of the request did not give any result:

```
----->
$ telnet www.springporttwppd.com 80
Trying 67.18.224.74...
Connected to www.springporttwppd.com.
Escape character is '^]'.
GET /helpdesk/admin_main.php HTTP/1.1
Host: www.springporttwppd.com
User-Agent: Mozilla/5.0 (X11; U; Linux i686; de-DE; rv:1.7.10)
Gecko/20050809 Firefox/1.0.6
Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: de,de-de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: UTF-8,*
Keep-Alive: 300
Connection: keep-alive
Authorization: Basic YWRtaW5pc3RyYXRvcjoxMjM0

HTTP/1.1 401 Authorization Required
Date: Tue, 30 Aug 2005 12:48:43 GMT
Server: Apache
WWW-Authenticate: Basic realm="Restricted Area"
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html

24e
[...]
Connection closed by foreign host.
<-----
```

Is it possible the effect is caused by your local or server setup (e.g. browser cache, webserver authentication setup...)?

Thomas Krüger