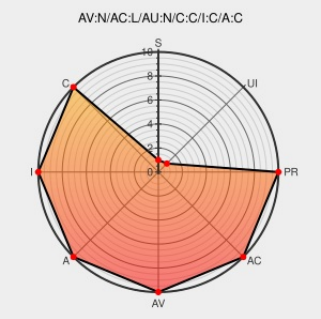
CVE-2013-6026

Published on: 10/19/2013 12:00:00 AM UTC

Last Modified on: 04/26/2023 06:55:00 PM UTC

CVE-2013-6026

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Vdsl Asl-55052 from Alphanetworks contain the following vulnerability:

The web interface on D-Link DIR-100, DIR-120, DI-624S, DI-524UP, DI-604S, DI-604UP, DI-604+, and TM-G5240 routers; Planex BRL-04R, BRL-04UR, and BRL-04CW routers; and Alpha Networks routers allows remote attackers to bypass authentication and modify settings via an xmlset_roodkcableoj28840ybtide User-Agent HTTP header, as exploited in the wild in October 2013.

CVE-2013-6026 has been assigned by cert@cert.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Reverse Engineering a D-Link Backdoor - /dev/ttyS0	Exploit www.devttys0.com text/html	MISC www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/
D-Link UK | Update on Router Security issue	www.dlink.com text/html	CONFIRM www.dlink.com/uk/en/support/security
Vulnerability Note VU#248083 - D-Link routers authenticate administrative access using specific User-Agent string	US Government Resource www.kb.cert.org text/html	CERT-VN VU#248083

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further

are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Alphanetworks	Vdsl Asl-55052	-	All	All	All
Hardware	Alphanetworks	Vdsl Asl-55052	-	All	All	All
Hardware	Alphanetworks	Vdsl Asl-56552	-	All	All	All
Hardware	Alphanetworks	Vdsl Asl-56552	-	All	All	All
Hardware	D-link	Di-524up	-	All	All	All
Hardware	D-link	Di-524up	-	All	All	All
Hardware	D-link	Di-604	-	All	All	All
Hardware	D-link	Di-604s	-	All	All	All
Hardware	D-link	Di-604s	-	All	All	All
Hardware	D-link	Di-604up	-	All	All	All
Hardware	D-link	Di-604up	-	All	All	All
Hardware	D-link	Di-604	-	All	All	All
Hardware	D-link	Di-604	-	All	All	All
Hardware	D-link	Di-624s	-	All	All	All
Hardware	D-link	Di-624s	-	All	All	All
Hardware	D-link	Dir-100	-	All	All	All
Hardware	D-link	Dir-100	-	All	All	All
Hardware	D-link	Dir-120	-	All	All	All
Hardware	D-link	Dir-120	-	All	All	All
Hardware	D-link	Tm-g5240	-	All	All	All
Hardware	D-link	Tm-g5240	-	All	All	All
Hardware	Dlink	Di-524up	-	All	All	All
Hardware	Dlink	Di-604s	-	All	All	All
Hardware	Dlink	Di-604up	-	All	All	All
Hardware	Dlink	Di-604	-	All	All	All
Hardware	Dlink	Di-624s	-	All	All	All

Hardware	Dlink	Dir-100	-	All	All	All
Hardware	Dlink	Dir-120	-	All	All	All
Hardware	Dlink	Tm-g5240	-	All	All	All
Hardware	Planex	Brl-04cw	-	All	All	All
Hardware	Planex	Brl-04cw	-	All	All	All
Hardware	Planex	Brl-04r	-	All	All	All
Hardware	Planex	Brl-04r	-	All	All	All
Hardware	Planex	Brl-04ur	-	All	All	All
Hardware	Planex	Brl-04ur	-	All	All	All

cpe:2.3:h:alphanetworks:vdsl_asl-55052:-:*:*:*:*:*:*:*:

cpe:2.3:h:alphanetworks:vdsl_asl-55052:-:*:*:*:*:*:*:*:

cpe:2.3:h:alphanetworks:vdsl_asl-56552:-:*:*:*:*:*:*:*:

cpe:2.3:h:alphanetworks:vdsl_asl-56552:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-524up:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-524up:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604+:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604s:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604s:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604up:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604up:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604\+:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-604\+:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-624s:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:di-624s:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-100:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-100:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-120:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:dir-120:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:tm-g5240:-:*:*:*:*:*:*:*:

cpe:2.3:h:d-link:tm-g5240:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:di-524up:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:di-604s:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:di-604up:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:di-604\+:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:di-624s:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dir-100:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:dir-120:-:*:*:*:*:*:*:*:

cpe:2.3:h:dlink:tm-g5240:-:*:*:*:*:*:*:*:

cpe:2.3:h:planex:brl-04cw:-:*:*:*:*:*:*:*:

cpe:2.3:h:planex:brl-04cw:-:*:*:*:*:*:*:*:

cpe:2.3:h:planex:brl-04r:-:*:*:*:*:*:*:*:

cpe:2.3:h:planex:brl-04r:-:*:*:*:*:*:*:*:

cpe:2.3:h:planex:brl-04ur:-:*:*:*:*:*:*:*:

cpe:2.3:h:planex:brl-04ur:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report