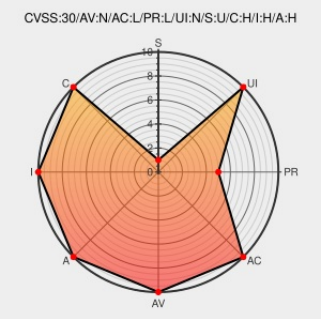
CVE-2017-18372

Published on: 05/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:54 PM UTC

CVE-2017-18372

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



Certain versions of 5200w-t from Billion contain the following vulnerability:

The Billion 5200W-T TCLinux Fw $7.3.8.0 v008 130603 router distributed by TrueOnline has a command injection vulnerability in the Time Setting function, which is only accessible by an authenticated user. The vulnerability is in the tools_time.asp page and can be exploited through the uiViewSNTPServer parameter. Authentication can be achieved by exploiting CVE-2017-18373.

CVE-2017-18372 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
	Exploit Third Party Advisory	MISC raw.githubusercontent.com/pedrib/PoC/master/advisories/zyxel_trueonline.txt

	raw.githubusercontent.com text/plain	
Full Disclosure: Multiple RCE in ZyXEL / Billion / TrueOnline routers	Exploit Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/fulldisclosure/2017/Jan/40
SSD Advisory - ZyXEL / Billion Multiple Vulnerabilities - SSD Secure Disclosure	Exploit Technical Description Third Party Advisory ssd-disclosure.com text/html	MISC ssd-disclosure.com/index.php/archives/2910

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Billion	5200w-t	-	All	All	All
Hardware	Billion	5200w-t	-	All	All	All
Operating System	Billion	5200w-t Firmware	7.3.8.0	All	All	All
Operating System	Billion	5200w-t Firmware	7.3.8.0	All	All	All
Hardware	Zyxel	P660hn-t1a V1	-	All	All	All
Hardware	Zyxel	P660hn-t1a V1	-	All	All	All
Operating System	Zyxel	P660hn-t1a V1 Firmware	7.3.15.0	All	All	All
Operating System	Zyxel	P660hn-t1a V1 Firmware	7.3.15.0	All	All	All
Hardware	Zyxel	P660hn-t1a V2	-	All	All	All
Hardware	Zyxel	P660hn-t1a V2	-	All	All	All
Operating System	Zyxel	P660hn-t1a V2 Firmware	7.3.15.0	All	All	All
Operating System	Zyxel	P660hn-t1a V2 Firmware	7.3.15.0	All	All	All

cpe:2.3:h:billion:5200w-t:-:*:*:*:*:*:*:*:

cpe:2.3:h:billion:5200w-t:-:*:*:*:*:*:*:*:

cpe:2.3:o:billion:5200w-t_firmware:7.3.8.0:*:*:*:*:*:*:*:

cpe:2.3:o:billion:5200w-t_firmware:7.3.8.0:*:*:*:*:*:*:*:

cpe:2.3:h:zyxel:p660hn-t1a_v1:-:*:*:*:*:*:*:*:

cpe:2.3:h:zyxel:p660hn-t1a_v1:-:*:*:*:*:*:*:*:

cpe:2.3:o:zyxel:p660hn-t1a_v1_firmware:7.3.15.0:*:*:*:*:*:*:*:

cpe:2.3:o:zyxel:p660hn-t1a_v1_firmware:7.3.15.0:*:*:*:*:*:*:*:

cpe:2.3:h:zyxel:p660hn-t1a_v2:-:*:*:*:*:*:*:*:

cpe:2.3:h:zyxel:p660hn-t1a_v2:-:*:*:*:*:*:*:*:

cpe:2.3:o:zyxel:p660hn-t1a_v2_firmware:7.3.15.0:*:*:*:*:*:*:*:

cpe:2.3:o:zyxel:p660hn-t1a_v2_firmware:7.3.15.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→