



CVE-2017-18371

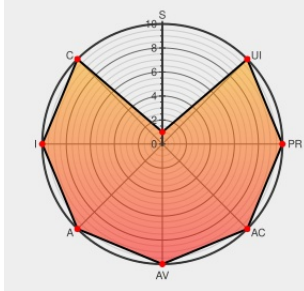
Published on: 05/02/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:55 PM UTC

CVE-2017-18371

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



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

The ZyXEL P660HN-T1A v2 TCLinux Fw #7.3.37.6 router distributed by TrueOnline has three user accounts with default passwords, including two hardcoded service accounts: one with the username true and password true, and another with the username supervisor and password zyad1234. These accounts can be used to login to the web

interface, exploit authenticated command injections, and change router settings for malicious purposes.

CVE-2017-18371 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	CVE-2017-18371	MISC

Exploit
Third Party Advisory
raw.githubusercontent.com
text/plain

MISC
raw.githubusercontent.com/pedrib/PoC/master/advisories/zyxel_trueonline.txt

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

New Mirai Variant Targets Enterprise Wireless Presentation & Display Systems

Technical Description
Third Party Advisory
unit42.paloaltonetworks.com
text/html

MISC unit42.paloaltonetworks.com/new-mirai-variant-targets-enterprise-wireless-presentation-display-systems/

Zyxel statement regarding unauthenticated remote command execution vulnerability | Zyxel

Broken Link
www.zyxel.com
text/html

ZYXEL MISC www.zyxel.com/support/announcement_unauthenticated.shtml

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

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, 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 	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	7.3.37.6	All	All	All
Operating System	Zyxel	P660hn-t1a V1 Firmware	7.3.37.6	All	All	All
Hardware 	Zyxel	P660hn-t1a V2	-	All	All	All
Hardware 	Zyxel	P660hn-t1a V2	-	All	All	All
Operating	Zyxel	P660hn-t1a V2 Firmware	7.3.37.6	All	All	All

System						
Operating System	Zyxel	P660hn-t1a V2 Firmware	7.3.37.6	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:7.3.37.6:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:zyxel:p660hn-t1a_v1_firmware:7.3.37.6:~::~~::~~::~~::~~::~~::~~:::						
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:7.3.37.6:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:zyxel:p660hn-t1a_v2_firmware:7.3.37.6:~::~~::~~::~~::~~::~~::~~:::						
No vendor comments have been submitted for this CVE						
← Previous ID			Next ID →			