

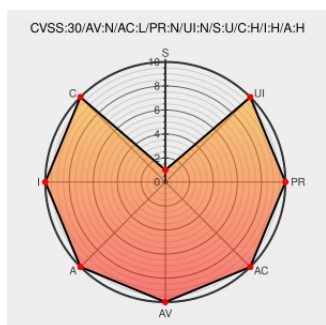


CVE-2018-1164

Published on: 02/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:32 PM UTC

CVE-2018-1164

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

Certain versions of [P-870h-51](#) from [Zyxel](#) contain the following vulnerability:

This vulnerability allows remote attackers to cause a denial-of-service condition on vulnerable installations of ZyXEL P-870H-51 DSL Router 1.00(AWG.3)D5. Authentication is not required to exploit this vulnerability. The specific flaw exists within numerous exposed CGI endpoints. The vulnerability is caused by improper access controls that allow access to critical functions without authentication. An attacker can use this vulnerability to reboot affected devices, along with other actions. Was ZDI-CAN-4540.

CVE-2018-1164 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **ZyXEL - ZyXEL P-870H-51 DSL Router** version **1.00(AWG.3)D5**

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: **10 - HIGH**

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

CVE References

Description

ZDI-18-135 | Zero Day Initiative

Tags

Third Party Advisory

VDB Entry

zerodayinitiative.com

text/html

Link

 MISC zerodayinitiative.com/advisories/ZDI-18-135

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  	Zyxel	P-870h-51	-	All	All	All
Hardware  	Zyxel	P-870h-51	-	All	All	All
Operating System	Zyxel	P-870h-51 Firmware	1.00(awg.3)d5	All	All	All
Operating System	Zyxel	P-870h-51 Firmware	1.00\awg.3\ d5	All	All	All
Operating System	Zyxel	P-870h-51 Firmware	1.00\awg.3\ d5	All	All	All
cpe:2.3:h:zyxel:p-870h-51:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:zyxel:p-870h-51:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:zyxel:p-870h-51_firmware:1.00(awg.3)d5:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:zyxel:p-870h-51_firmware:1.00\awg.3\ d5:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:zyxel:p-870h-51_firmware:1.00\awg.3\ d5:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →