

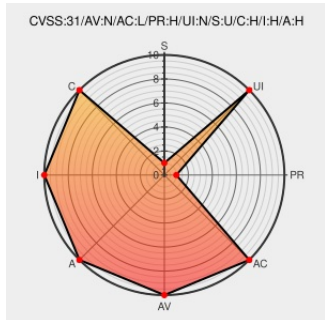


CVE-2020-8958

Published on: 07/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:00 PM UTC

CVE-2020-8958

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

Certain versions of [1ge 3fe Wifi Onu V2804rgw](#) from [Gpononu](#) contain the following vulnerability:

Guangzhou 1GE ONU V2801RW 1.9.1-181203 through 2.9.0-181024 and V2804RGW 1.9.1-181203 through 2.9.0-181024 devices allow remote attackers to execute arbitrary OS commands via shell metacharacters in the boaform/admin/formPing Dest IP Address field.

CVE-2020-8958 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.2 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	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
GitHub - qurbat/gpon: A proof of concept for CVE-2020-8958 written in Python.	Exploit Third Party Advisory github.com text/html	MISC github.com/qurbat/gpon

V-SOL V2804EW 4GE GPON WIFI ONU	Product www.gpononu.com text/html	MISC www.gpononu.com/gpon-ont/4ge-epon-onu-v2804ew.html
1GE Router WiFi ONU(dual mode) EPON/GPON ONU	Product www.gpononu.com text/html	MISC www.gpononu.com/dual-mode-onu/1GE-Router-WiFi-ONU.html
Arbitrary OS command injection on V-SOL home routers – Karan Saini	Exploit Third Party Advisory www.karansaini.com text/html	MISC www.karansaini.com/os-command-injection-v-sol/

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

Exploit/POC from Github

CVE-2020-8958: Authenticated RCE exploit for NetLink HG323

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Gpononu	1ge 3fe Wifi Onu V2804rgw	-	All	All	All
Hardware 	Gpononu	1ge 3fe Wifi Onu V2804rgw	-	All	All	All
Operating System	Gpononu	1ge 3fe Wifi Onu V2804rgw Firmware	All	All	All	All
Hardware 	Gpononu	1ge Router Wifi Onu V2801rw	-	All	All	All
Hardware 	Gpononu	1ge Router Wifi Onu V2801rw	-	All	All	All
Operating System	Gpononu	1ge Router Wifi Onu V2801rw Firmware	All	All	All	All
cpe:2.3:h:gpononu:1ge\+3fe\+wifi_onu_v2804rgw:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:gpononu:1ge\+3fe\+wifi_onu_v2804rgw:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:gpononu:1ge\+3fe\+wifi_onu_v2804rgw_firmware:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:gpononu:1ge_router_wifi_onu_v2801rw:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:gpononu:1ge_router_wifi_onu_v2801rw:-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:gpononu:1ge_router_wifi_onu_v2801rw_firmware:~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @ipssignatures	It's new to me that proofpoint has a protection/signature/rule for the vulnerability CVE-2020-8958.... twitter.com/i/web/status/1...	2021-11-18 02:02:01
 @ipssignatures	It is the first time for me to know a protection/signature/rule for the vulnerability CVE-2020-8958. #Se7ssrwq6kcgna	2021-11-18 02:02:01
 @sylvaincortes	? Le malware BotenaGo infecte les routeurs et les objets connectés. ► Exploitation notamment de la CVE-2020-8958 ►... twitter.com/i/web/status/1...	2021-12-06 09:45:57
 @F5Labs	In August CVE-2020-8958 continued its run as the most frequently targeted vulnerability in our sensor logs, along w... twitter.com/i/web/status/1...	2022-09-22 17:55:39
 @F5Labs	In August CVE-2020-8958 continued its run as the most frequently targeted vulnerability in our sensor logs, along w... twitter.com/i/web/status/1...	2022-09-27 08:29:16
 @F5Labs	In August CVE-2020-8958 continued its run as the most frequently targeted vulnerability in our sensor logs, along w... twitter.com/i/web/status/1...	2022-10-01 16:30:59
 @F5Labs	CVE-2020-8958 was the top targeted vulnerability in our logs in November 2022. Learn which other vulnerabilities ar... twitter.com/i/web/status/1...	2022-12-23 18:30:58
 @JacslsLee	CVE-2020-8958 was the top targeted vulnerability in our logs in November 2022. Learn which other vulnerabilities ar... twitter.com/i/web/status/1...	2022-12-27 09:09:35
 @grabera7	CVE-2020-8958 was the top targeted vulnerability in our logs in November 2022. Learn which other vulnerabilities ar... twitter.com/i/web/status/1...	2022-12-27 19:49:39
 @CujoaiLabs	@malwrhunterteam Botnet moves first to 45.12.253.12, then 45.9.74.88. Adds exploits for: CVE- 2020-8958 CVE-2022-229... twitter.com/i/web/status/1...	2023-02-08 15:33:28

[← 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 registered 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](#)