

# Zyxel Routers and Home WiFi Systems - Unprotected Root Access via UART Using Default Password

High

[← View More Research Advisories](#)

## Synopsis

On Zyxel models NBG6818, NBG7815, WSQ20, WSQ50, WSQ60, and WSR30, the UART port on the PCB board gives a root BusyBox shell that prompts for a non-user configurable hardcoded default password present in a configuration file on the firmware (/etc/uci\_defconfig/system):

```
/etc/uci_defconfig/system:
option pwd "nbg6818@2019"
option gui_pwd "1234"
option language "en"
```

For this particular model (NBG6818), the default password is "nbg6818@2019". Other affected models will have different default passwords.

## Solution

See vendor advisory for instructions on how to update to patched firmware.

## Additional References

[https://www.zyxel.com/support/ZyxeL\\_security\\_advisory\\_for\\_pre-configured\\_password\\_management\\_vulnerability\\_of\\_home\\_routers\\_and\\_WiFi\\_systems.shtml](https://www.zyxel.com/support/ZyxeL_security_advisory_for_pre-configured_password_management_vulnerability_of_home_routers_and_WiFi_systems.shtml)

## Disclosure Timeline

8/25/2021 - Vendor Alerted  
8/25/2021 - Vendor Acknowledged  
8/26/2021 - Vendor asked for more information  
8/26/2021 - Tenable responded  
8/30/2021 - Zyxel responds and plans to assign CVE  
9/3/2021 - Zyxel informs they plan to disclose on November 23  
9/27/2021 - Zyxel asks for disclosure link information  
10/5/2021 - Tenable responds with disclosure link information  
11/23/2021 - Zyxel release patches

*All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.*

*Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.*

*For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.*

*If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)*

## Risk Information

**CVE ID:** [CVE-2021-35033](#)

**Tenable Advisory ID:** TRA-2022-06

**Credit:** Nicholas Miles

**CVSSv3 Base / Temporal Score:** 7.8/7.0

**CVSSv3 Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Additional Keywords:** zyxel  
uart

**Affected Products:** NBG6818  
NBG7815  
WSQ20  
WSQ50  
WSQ60  
WSR30

**Risk Factor:** High

## Advisory Timeline

2/28/2022 - Advisory published

[Tenable.io Web App Scanning](#)

[Tenable.asm External Attack Surface](#)

[Tenable.ad Active Directory](#)

[Tenable.ot Operational Technology](#)

[Tenable.sc Security Center](#)

[Tenable Lumin](#)

[Nessus](#)

[→ View all Products](#)

## FEATURED SOLUTIONS

[Application Security](#)

[Building Management Systems](#)

[Cloud Security Posture Management](#)

[Compliance](#)

[Exposure Management](#)

[Finance](#)

[Healthcare](#)

[IT/OT](#)

[Ransomware](#)

[State / Local / Education](#)

[US Federal](#)

[Vulnerability Management](#)

[Zero Trust](#)

[→ View all Solutions](#)

## CUSTOMER RESOURCES

[Resource Library](#)

[Community & Support](#)

[Customer Education](#)

[Tenable Research](#)

[Documentation](#)

[Trust and Assurance](#)

[Nessus Resource Center](#)

[Cyber Exposure Fundamentals](#)

[System Status](#)

## CONNECTIONS

[Blog](#)

[Contact Us](#)

[Careers](#)

[Investors](#)

[Events](#)

[Media](#)