# CVE Detail – CVE-2021-35033

A vulnerability in specific versions of Zyxel NBG6818, NBG7815, WSQ20, WSQ50, WSQ60, and WSR30 firmware with pre-configured password management could allow an attacker to obtain root access of the device, if the local attacker dismantles the device and uses a USB-to-UART cable to connect the device, or if the remote assistance feature had been enabled by an authenticated user.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.08779

## CVSS Scoring

CVSS v3.1 Score: 7.8

Severity: HIGH

## Mapped CWE(s)

* CWE-260: Password in Configuration File
* CWE-287: Improper Authentication

## CAPEC(s)

* CAPEC-114: Authentication Abuse
* CAPEC-115: Authentication Bypass
* CAPEC-151: Identity Spoofing
* CAPEC-194: Fake the Source of Data
* CAPEC-22: Exploiting Trust in Client
* CAPEC-57: Utilizing REST's Trust in the System Resource to Obtain Sensitive Data
* CAPEC-593: Session Hijacking
* CAPEC-633: Token Impersonation
* CAPEC-650: Upload a Web Shell to a Web Server
* CAPEC-94: Adversary in the Middle (AiTM)

## ATT&CK Techniques

* T1557: Adversary-in-the-Middle
* T1040: Network Sniffing
* T1185: Browser Session Hijacking
* T1563: Remote Service Session Hijacking
* T1505.003: Web Shell
* T1548: Abuse Elevation Control Mechanism
* T1134: Access Token Manipulation
* T1550.001: Application Access Token

## Used By (Actors/Tools)

* TrickBot (malware)
* cd00r (malware)
* JumbledPath (malware)
* SEASHARPEE (malware)
* VersaMem (malware)
* reGeorg (malware)
* Ursnif (malware)
* AppleSeed (malware)
* BUSHWALK (malware)
* J-magic (malware)
* SslMM (malware)
* Emotet (malware)
* Mafalda (malware)
* P.A.S. Webshell (malware)
* TRANSLATEXT (malware)
* Regin (malware)
* Line Dancer (malware)
* Raspberry Robin (malware)
* BlackCat (malware)
* IcedID (malware)
* GLASSTOKEN (malware)
* ASPXSpy (malware)
* China Chopper (malware)
* SnappyTCP (malware)
* LIGHTWIRE (malware)
* Line Runner (malware)
* Duqu (malware)
* Cuba (malware)
* FoggyWeb (malware)
* Hydraq (malware)
* CreepyDrive (malware)
* Chaes (malware)
* Sagerunex (malware)
* RAPIDPULSE (malware)
* MegaCortex (malware)
* Grandoreiro (malware)
* PULSECHECK (malware)
* MESSAGETAP (malware)
* XLoader (malware)
* Ryuk (malware)
* HermeticWiper (malware)
* OwaAuth (malware)
* Cobalt Strike (malware)
* SUPERNOVA (malware)
* Neo-reGeorg (malware)
* Carberp (malware)
* FRAMESTING (malware)
* SUNSPOT (malware)
* WIREFIRE (malware)
* STEADYPULSE (malware)
* SLIGHTPULSE (malware)
* Penquin (malware)
* Melcoz (malware)
* KillDisk (malware)
* Agent Tesla (malware)
* QakBot (malware)
* Gelsemium (malware)
* Dridex (malware)
* Dok (malware)
* NPPSPY (tool)
* Sliver (tool)
* PowerSploit (tool)
* Impacket (tool)
* Empire (tool)
* PoshC2 (tool)
* Peirates (tool)
* Responder (tool)
* NBTscan (tool)
* Operation Wocao (campaign)
* Velvet Ant (intrusion-set)
* APT41 DUST (campaign)
* ArcaneDoor (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Operation CuckooBees (campaign)
* Sandworm Team (intrusion-set)
* Ember Bear (intrusion-set)
* FIN6 (intrusion-set)
* APT28 (intrusion-set)
* Volt Typhoon (intrusion-set)
* Magic Hound (intrusion-set)
* APT29 (intrusion-set)
* HAFNIUM (intrusion-set)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* APT32 (intrusion-set)
* APT5 (intrusion-set)
* BackdoorDiplomacy (intrusion-set)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* Tropic Trooper (intrusion-set)
* 2015 Ukraine Electric Power Attack (campaign)
* Moses Staff (intrusion-set)
* DarkVishnya (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* CURIUM (intrusion-set)
* Blue Mockingbird (intrusion-set)
* Versa Director Zero Day Exploitation (campaign)
* BlackByte (intrusion-set)
* Threat Group-3390 (intrusion-set)
* Tonto Team (intrusion-set)
* Agrius (intrusion-set)
* Sea Turtle (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* Salt Typhoon (intrusion-set)
* C0032 (campaign)
* HomeLand Justice (campaign)
* C0017 (campaign)
* APT33 (intrusion-set)
* Cutting Edge (campaign)
* Lotus Blossom (intrusion-set)
* Volatile Cedar (intrusion-set)
* 2022 Ukraine Electric Power Attack (campaign)
* Deep Panda (intrusion-set)
* FrostyGoop Incident (campaign)

## Affected Products

* cpe:2.3:o:zyxel:nbg6818\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:zyxel:nbg7815\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:zyxel:wsq20\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:zyxel:wsq50\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:zyxel:wsq60\_firmware:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:zyxel:wsr30\_firmware:\*:\*:\*:\*:\*:\*:\*:\*