Critical flaws in Chinese robots. A zombie robot bonet can be remotely co

Data: 2025-09-28 16:12:36

Autor: Inteligência Against Invaders

Redazione RHC**:28 September 2025 18:12**

On September 27, 2025, new concerns emerged about robots produced by China's Unitree Robotics , after serious vulnerabilities were reported that could expose thousands of devices to remote control and malicious use.

According to *IEEE Spectrum* on Thursday, September 25, researchers have discovered **a critical flaw in the Bluetooth Low Energy (BLE) system used by the company's robots** for initial Wi-Fi network setup. This weakness *would allow an attacker to gain root privileges on the devices' Android operating system, gaining complete control over them.*

Security researcher Andreas Makris explained that once a robot is compromised, *the infection can automatically spread to other Yushu devices* within Bluetooth range, turning them into a botnet capable of replicating without human intervention.

The authentication mechanism appears particularly fragile: *Unitree robots allow access simply by encrypting a hardcoded string, "unitree."* This **allows an attacker to insert arbitrary code disguised as the WiFi network's SSID and password.** When the robot attempts to connect, *the code would be executed with administrator privileges, without any additional verification.*

Makris added that **such an exploit could even prevent users from updating their firmware,** leaving devices permanently vulnerable and opening the door to mass takeover. **Affected models include the Go2 and B2 quadruped robot dogs and the G1 and H1 humanoid robots** . This is the first time a flaw of this magnitude has been publicly disclosed on a commercial humanoid robotics platform.

Researchers contacted *Unitree Robotics as early as May 2025, but after several unsuccessful attempts to communicate, the company reportedly stopped responding last July.* The lack of cooperation prompted the public disclosure of the vulnerability. Makris also noted that **he had previously identified a backdoor in the Yushu Go1 model,** raising questions about the origin of these flaws: whether they are *the result of negligent development or intentional implementations.*

A further report came from **Victor Mayoral-Vilches** , founder of Alias Robotics, who claimed that Yushu robots *are sending telemetry data to Chinese servers, which could include audio, video, and spatial information* . Mayoral-Vilches highlighted how these devices **are widely used globally, but many users are unaware of the risks associated with their use** . While awaiting official responses, the expert advises users to connect the robots only to isolated Wi-Fi networks and to disable Bluetooth connectivity as an immediate protection measure.

The concerns aren’t limited to personal matters. In August 2025, **the city of Taipei deployed the Go2 model for urban patrol, raising questions about data security.** On May 5, 2025, the U.S. House of Representatives Special Committee on Strategic Competition with China *sent a letter to the Secretary of Defense, the Secretary of Commerce, and the Chairman of the Federal Communications Commission, warning that Yushu “poses a growing threat to national security.”*

The company’s robots have reportedly already been deployed in sensitive environments *such as prisons, police forces, and US military bases. The presence of backdoors and the possibility of remote surveillance have led some observers to call them “Trojan horses with cameras.”*

To date, Unitree Robotics has not released any official comment.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli