Critical Baicells Device Vulnerability Can Expose Telecoms Networks to Snooping



A critical vulnerability affecting wireless communication base stations from Baicells Technologies can be exploited to cause disruption in telecom networks or take complete control of data and voice traffic, according to a researcher.

Baicells Technologies is a US-based telecommunications equipment provider for 4G and 5G networks. The company says more than 100,000 of its base stations are deployed across 64 countries around the world.

Cyber offensive researcher Rustam Amin discovered that at least some of Baicells' Nova base station products are affected by a critical command injection vulnerability that can be exploited remotely without authentication by sending specially crafted HTTP requests to the targeted device.

Exploitation of the vulnerability, tracked as CVE-2023-24508,

can allow an attacker to run shell commands with root privileges and take complete control of a device, Amin told SecurityWeek.

The researcher explained that an attacker could, for instance, easily shut down a device to cause disruption. In addition, they could take full control over the traffic and phone calls going over a targeted network. A hacker could obtain information such as phone numbers, IMEI, and location data.

However, conducting such an attack is not an easy task and it requires specific knowledge of the targeted network.

Amin told SecurityWeek that there are more than 1,150 devices exposed to the internet, mostly located in the United States.

Baicells published an advisory to inform customers about the vulnerability on January 24. The researcher said the vendor was quick to respond to his notification and quick to issue a patch.

Nova 227, 233, 243 and 246 base stations are affected. The security hole has been patched with the release of version 3.7.11.3.

The vendor’s advisory only mentions Nova products as being impacted, but the researcher believes other products could be impacted as well.

The US Cybersecurity and Infrastructure Security Agency (CISA) published an advisory last week to inform organizations about CVE-2023-24508.

Amin recently also discovered serious vulnerabilities in Econolite EOS traffic controller software, which can be exploited to control traffic lights.

Related: OT Security Firm Warns of Safety Risks Posed by Alerton Building System Vulnerabilities

Related: US Details Chinese Attacks Against Telecoms Providers

Related: Cisco Patches High-Severity Vulnerabilities in Communications, Networking Products

https://www.securityweek.com/critical-baicells-device-vulnerability-can-expose-telecoms-networks-to-snooping/