CERT-In Vulnerability Note CIVN-2025-0005

Security Misconfiguration Vulnerability in CP Plus Router

Original Issue Date:January 20, 2025

Severity Rating: HIGH

Systems Affected

- CP Plus CP-XR-DE21-S Router - firmware version DE21_S_india_hx806_1.057.043_0023

Overview

A vulnerability has been reported in CP Plus Router, which could allow an attacker to obtain sensitive information and compromise the targeted system.

Target Audience:
End-users/ Administrators of CP Plus CP-XR-DE21-S Router.

Risk Assessment:
Session Hijacking, or Man-in-the-Middle (MITM) attacks on targeted device.

Impact Assessment:
Impact on confidentiality, integrity and availability of the vulnerable device.

Description

The CP Plus CP-XR-DE21-S is a 4G LTE router designed for high-speed internet connectivity, suitable for home and small-office use.

This vulnerability exists in the CP Plus Router due to insecure handling of cookie flags used within its web interface. A remote attacker could exploit this vulnerability by intercepting data transmissions during an HTTP session on the vulnerable system.

Successful exploitation of this vulnerability could allow the attacker to obtain sensitive information and compromise the targeted system.

Credit

This vulnerability is reported by Shravan Singh and Karan Patel from Redfox Cyber Security.

Solution

Upgrade CP Plus CP-XR-DE21-S Router to firmware version DE21_S_india_hx806_1.057.043_0027
https://cpplusworld.com/firmware

Vendor Information

CP-Plus
https://cpplusworld.com/firmware

References

CP-Plus
https://cpplusworld.com/firmware

CVE Name

CVE-2025-0479

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-22902657

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India