

HOME

ABOUT CERT-In

KNOWLEDGEBASE


TRAINING

ADVISORIES

VULNERABILITY NOTES

CYBER SECURITY
ASSURANCE






साइबर स्वच्छता केन्द्र


CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre


Full Member




Operational Member




Accredited Member



Global Research Partner



Associate Partner



Directions by CERT-In under Section 70B, Information Technology Act 2000

Guidelines on Information Security Practices for Government Entities

Technical Guidelines on SOFTWARE BILL OF MATERIALS (SBOM)

ABOUT CERT-In

- Client's /Citizen's Charter
- Roles & Functions
- Advisory Committee
- Act/Rules/Regulations
- Internal Complaint Committee (ICC)
- RFC2350
- Press
- Tender
- Subscribe Mailing List
- Contact Us

REPORTING

- Incident Reporting
- Vulnerability Reporting
- Feedback

KNOWLEDGEBASE

- Guidelines
- Presentations
- White Papers
- Annual Report

RECRUITMENTS

Security Tips for Common Users

ADVISORIES

VULNERABILITY NOTES

RELATED LINKS

- World CERTs
- Antivirus Resources
- FAQ

Home - Vulnerability Notes

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

Performance Management

india.gov.in

Public Grievances (DAR&PG)

मेरी सरकार

Open Government Data (OGD) Platform India

ISAC Power

NEW

राष्ट्रीय मतदाता सेवा पोर्टल
NATIONAL VOTERS' SERVICES PORTAL
www.eci.nic.in | www.nvsp.in

Modes of Digital Payments

DIGITAL PAYMENT

इराक़्हा

RTI

Collaboration and Engaging with CERT-In

NEW

State/Sectoral CSIRT

NEW

Indian Computer Emergency Response Team - CERT-In, Ministry of Electronics and Information Technology, Government of India.

[Website Policies](#) | [Terms of Use](#) | [Help](#)

Last Updated On January 26, 2025