مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in D-Link Routers

Tracking #:432316294

Date:17-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in D-Link routers that could be exploited to gain unauthorized access to devices, execute malicious code, and potentially take full control.

TECHNICAL DETAILS:

Vulnerabilities Details:

1. **CVE-2024-45694 (CVSS 9.8) – Stack-based Buffer Overflow**
   - Affects:
     - DIR-X5460 A1 (firmware versions 1.01, 1.02, 1.04, 1.10)
     - DIR-X4860 A1 (firmware versions 1.00, 1.04)
   - Impact: Allows unauthenticated remote attackers to execute arbitrary code on the device.
2. **CVE-2024-45698 (CVSS 8.8) – OS Command Injection**
   - Affects:
     - DIR-X4860 A1 (firmware versions 1.00, 1.04)
   - Impact: Attackers can access the router via telnet using hard-coded credentials and execute arbitrary OS commands.
3. **CVE-2024-45697 (CVSS 9.8) – Hidden Functionality**
   - Affects:
     - DIR-X4860 A1 (firmware versions 1.00, 1.04)
   - Impact: Telnet service enabled by default when WAN port connects, allowing remote command execution.
4. **CVE-2024-45695 (CVSS 9.8) – Stack-based Buffer Overflow (DIR-X4860 A1)**
   - Affects:
     - DIR-X4860 A1 (firmware versions 1.00, 1.04)
   - Impact: Unauthenticated remote access leading to arbitrary code execution.
5. **CVE-2024-45696 (CVSS 8.8) – Hidden Functionality with Internal Access**
   - Affects:
     - DIR-X4860 A1 (firmware versions 1.00, 1.04)
     - COVR-X1870 (firmware versions v1.02 and earlier)
   - Impact: Allows enabling telnet service via specific network packets, posing risks in local networks.

Fixed Firmware Versions:

- **DIR-X5460 A1:** Update to version **1.11B04 or later**
- **DIR-X4860 A1:** Update to version **1.04B05 or later**
- **COVR-X1870:** Update to version **v1.03B01 or later**

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10412