COMMUNITY CONTENT

Submit #791217: Tenda i12 V1.0.0.11(3862) Path Traversal

Title	Tenda i12 V1.0.0.11(3862) Path Traversal
Description	A critical authentication bypass vulnerability exists in the Tenda i12 V1.0.0.11(3862) router, specifically within the R7WebsSecurityHandlerfunction of the V1.0.0.11(3862) firmware. This function acts as a security gatekeeper for all incoming HTTP requests. Its primary mechanism is a URL prefix whitelist (e.g., /public/, /lang/) meant to grant unauthenticated access to static resources. The function uses strncmp to check if the request URL begins with these trusted prefixes: e.g., if (!strncmp(s1, "/public/", 8u) ... return 0;However, the application fails to validate or canonicalize the subsequent part of the URL. An unauthenticated remote attacker can send a crafted HTTP request that starts with a whitelisted prefix but employs directory traversal sequences (../) to escape the restricted directory.For example, a request to /public/../system_upgrade.asp will satisfy the strncmp check (bypassing authentication) but will be resolved by the web server to the sensitive system_upgrade.asp page, granting full administrative access.
Source	⚠ https://github.com/Litengzheng/vuldb_new/blob/main/i12/vul_110/README.md
User	LtzHust2 (UID 95662)
Submission	03/27/2026 04:12 PM (13 days ago)
Moderation	04/08/2026 09:15 PM (12 days later)
Status	Accepted
VulDB entry	356375 [Tenda i12 1.0.0.11(3862) HTTP path traversal]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling