COMMUNITY CONTENT

Submit #789935: Tenda i3 V1.0.0.6(2204) Authentication Bypass Issues

Title	Tenda i3 V1.0.0.6(2204) Authentication Bypass Issues
Description	A critical authentication bypass vulnerability exists in the i3 V1.0.0.6(2204) firmware. The vulnerability is located in the `R7WebsSecurityHandler` function, which acts as the security filter for HTTP requests. The application defines a whitelist of URL prefixes (e.g., `/public/`, `/lang/`) that are allowed to be accessed without authentication. 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 `/lang/../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/MrXiaoFan/TendaVul/tree/main/tenda-i3-V1.0.0.6(2204)-R7WebsSecurityHandler-Authentication%20Bypass%20Issues
User	Fan95 (UID 95969)
Submission	03/26/2026 10:04 AM (14 days ago)
Moderation	04/08/2026 07:35 PM (13 days later)
Status	Accepted
VulDB entry	356297 [Tenda i3 1.0.0.6(2204) HTTP R7WebsSecurityHandler 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