مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SSRF Vulnerability in Better Auth SSO

Tracking #:432319294

Date:20-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical Server-Side Request Forgery (SSRF) vulnerability has been identified in the @better-auth/sso plugin used by the Better Auth authentication framework for TypeScript applications.

TECHNICAL DETAILS:

A critical Server-Side Request Forgery (SSRF) vulnerability, CVE-2026-53513 has been identified in the @better-auth/sso plugin used by the Better Auth authentication framework for TypeScript applications. The vulnerability allows an authenticated attacker to manipulate OpenID Connect (OIDC) provider registration and force the application server to send requests to internal or cloud-hosted services.
Successful exploitation may allow attackers to access sensitive internal resources, including cloud metadata services, Redis instances, and administrative interfaces that are not publicly accessible. In environments configured with trustEmailVerified: true, the vulnerability can also be leveraged to perform account takeover through malicious OAuth account linking.

Vulnerability Details:

- CVE ID: CVE-2026-53513
- Severity: Critical
- CVSS Score: 9.6 (CVSS v3.x)
- Vulnerability Type: Server-Side Request Forgery (SSRF)
- Affected Product: @better-auth/sso (Better Auth SSO Plugin)
- Affected Versions: = 0.1.0 and < 1.6.11
- Patched Version: 1.6.11
- Authentication Required: Yes (Authenticated user)

RECOMMENDATIONS:

Immediate Actions:

- Upgrade @better-auth/sso to fixed version or later.

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://github.com/better-auth/better-auth/security/advisories/GHSA-5rr4-8452-hf4v