ADVISORY

DATE

2 NOVEMBER 2020

ServiceStack <=5.9.1 JWT Signature Verification Bypass

Summary

ServiceStack is affected by a signature verification bypass in the `ServiceStack.Auth.JwtAuthProviderReader` method, which could be used to bypass the authentication mechanisms and/or to elevate privileges.

This security advisory is referred to a vulnerability found and resolved internally by ServiceStack's development team, read the "Re-discovering a JWT Authentication Bypass in ServiceStack" for more information.

Product Description (from vendor)

"ServiceStack is an open-source framework designed to be an alternative to the WCF, ASP.NET MVC, and ASP.NET Web API frameworks. It supports REST and SOAP endpoints, autoconfiguration of data formats, inversion of control containers, object-relational mapping, caching mechanisms, and much more." For more information visit https://servicestack.net/

CVE(s)

- CVE-2020-28042

Details

Root Cause Analysis

The verification of a `JWT` token consists of the server extracting the `header` and the `payload` of the token from a given request, re-calculating the signature server-side, and finally comparing the calculated signature with the one in the request through the `VerifyPayload` function.

The `VerifyPayload` function make usage of the following `ServiceStack.EnumerableUtils.EquivalentTo` method:

```
237 public static bool EquivalentTo(this byte[] bytes, byte[] other)
238     {
239         var compare = 0;
240         for (var i = 0; i < other.Length; i++)
241             compare |= other[i] ^ bytes[i];
242 
243         return compare == 0;
244     }
```

The method is called with the server-side generated signature as `bytes` and the request signature as `other`.
As no length check is performed and the check is pre-set to the success value (`var compare = 0`), it is possible to bypass the whole check by submitting an empty signature. If `other.Length` is `0` then no checks are performed and the function will always return `True`.

Proof of Concept

1. Create a web application that uses the ServiceStack JWT authentication provider before version 5.9.2.
2. Forge a valid token (or get one from the service).
3. Remove the signature from the token (e.g. `HEADER.PAYLOAD.SIGNATURE` becomes `HEADER.PAYLOAD.`).
4. Sent the tampered token to an authenticated API and notice that the token is correctly validated.

Impact

An attacker can forge a valid JWT token with arbitrary content.

Remediation

Upgrade ServiceStack to version 5.9.2 or later.

Disclosure Timeline

N/A

Credits

- mythz from ServiceStack for discovering and fixing the vulnerability
- Andrea `zi0black` Cappa from Shielder for the advisory

This advisory was first published on https://www.shielder.com/advisories/servicestack-jwt-signature-verification-bypass/

INFO

Shielder S.r.l.

P.I. 11435310013

REA TO - 1213132

Registered Capital: 81.000,00 €

Via Palestro, 1/C
10064 Pinerolo (TO) Italy

CONTACTS

info@shielder.com

Landline: (+39) 0121 - 39 36 42

Commercial: (+39) 345 - 30 31 983

Technical: (+39) 393 - 16 66 814