Title: Navigating the Modern Battlefront of JWT Security

**Submitted by: Viktor Mares, Sr Penetration Tester at SoCyber**

## **Description**

JSON Web Tokens (JWTs) have become omnipresent tools for web authentication, authorization, session management and identity federation. However, some have criticized JWT and associated Javascript Object Signing and Encryption (JOSE) standards for cryptographic design flaws and dangerous levels of complexity. These have arguably led to severe vulnerabilities such as the well-known “alg”:“none”

attack.

We will have a closer look at the JOSE standards and identify potential implementation mistakes that might result in vulnerabilities in JWT libraries if the RFCs are interpreted in certain ways. We will look at

three modern classes of JWT attacks that affected very widely used libraries (Authlib, JWCrypto & JWX). Two of these attacks (“sign/encrypt confusion” and “polyglot token”) can allow complete token forgery, allowing authentication bypasses or privilege escalation in applications using an affected library and configuration. The third (“billion hashes”) attack can be leveraged for a denial-of-service attack against

token-processing servers.

1. **Workshop (2 - 3h) – Hacking JWTs in modern APIs**

A 2-3 hour workshop, which will represent an API. It will allow anyone to authenticate, creating a unique JWT token (based on the username), but all users will be created as ‘NOTadmin’. The main goal will be to escalate privileges by forging a JWT token in order to become the ‘admin’ user of that API. The participants will need to derive the Public Key used for signing the JWTs and then use Burp Suite to sign their own forged JWTs.